Mode d'emploi
hybird 120 Gigaset Edition

Copyright© Version 1.0, 2013 Gigaset Communications GmbH

Note légale

Cette publication est sujette à changement. Gigaset GmbH n'offre aucune garantie que ce soit des informations contenues dans ce manuel. Gigaset GmbH n'est pas responsable des dommages directs, indirects, collatéraux, indirects ou tout autre relié à la livraison, la fourniture ou l'utilisation de ce manuel.

Copyright © Gigaset GmbH Tous les droits sur les données incluses, en particulier le droit de copier et de propager, sont resevered par Gigaset GmbH.

Table des matières

Chapitre 1 Assistants 1

Chapitre 2 Gestion du système 2

2.1 État 2

2.2 Paramètres globaux 4

2.2.1 Système 4

2.2.2 Mots de passe 10

2.2.3 Date et heure 13

2.2.4 Horloge 17

2.2.5 Licences système 19

2.3 Codes 20

2.3.1 Codes modifiables 20

2.4 Mode Interface / groupes Bridge 22

2.4.1 Interfaces 24

2.5 Accès administratif 25

2.5.1 Accès 25

2.5.2 SSH 26

2.5.3 SNMP 29

2.6 Authentification distante 30

2.6.1 RADIUS 30

2.6.2 TACACS+ 36

2.6.3 Options 39

2.7 Accès à la configuration 39

2.7.1 Profils d'accès 40

2.7.2 Utilisateur 42

2.8 Certificats 43

2.8.1 Liste de certificat 44

2.8.2 CRL 51
2.8.3 Serveur de certificat 52

Chapitre 3 Interfaces physiques 54

3.1 Ports Ethernet 54
3.1.1 Configuration du port 55

3.2 Ports RNIS 56
3.2.1 RNIS externe 57
3.2.2 RNIS interne 58

3.3 Ports analogiques 60
3.3.1 Analogue externe (FXO) 60
3.3.2 Analogue interne (FXS) 63

Chapitre 4 VoIP 64

4.1 Paramètres 64
4.1.1 Fournisseur SIP 64
4.1.2 Emplacements 73
4.1.3 Profils Codec 75
4.1.4 Options 78

Chapitre 5 Numérotation 80

5.1 Connexions externes 80
5.1.1 Connexions 80
5.1.2 Numéros d'appel 83
5.1.3 Groupage 85
5.1.4 X.31 86

5.2 Paramètres de l'utilisateur 88
5.2.1 Utilisateur 88
5.2.2 Classes d'autorisation 96
5.2.3 Appel en parallèle 111

5.3 Groupes et équipes 112
5.3.1 Teams 112

5.4 Répartition des appels 120
5.4.1 Affectation des appels 120
5.4.2 Rejet si numérotation erronée 123

Chapitre 6 Appareil terminal 125

6.1 Gigaset Téléphone 125
6.1.1 Gigaset Téléphone 125
6.1.2 Gigaset DECT 128

6.2 Autres téléphones 132
6.2.1 VoIP 132
6.2.2 RNIS 136
6.2.3 Analogue 137
6.2.4 CAPI 140

6.3 Aperçu 141
6.3.1 Aperçu 141

Chapitre 7 Contrôle d'appel 143

7.1 Services sortants 143
7.1.1 Appel direct 143
7.1.2 Transfert des appels (AWS) 144
7.1.3 Contrôle de numérotation 146
7.1.4 Numéro d'appel prioritaire 148

7.2 Règles de sélection 148
7.2.1 Général 149
7.2.2 Interfaces/Fournisseurs 150
7.2.3 Zones et routage 150

Chapitre 8 Applications 153

8.1 Calendrier 153
8.1.1 Calendrier 153
8.1.2 Jours fériés 157

8.2 Rejet 157
8.2.1 Fonctions de rejet 158
8.2.2 Applications du rejet 162

8.3 Application vocale 163
8.3.1 Fichiers wave 164

8.4 Répertoire téléphonique du système 165
8.4.1 Entrées 167
8.4.2 Importation / Exportation 168
8.4.3 Général 169

8.5 Données de connexion 170
8.5.1 Sortant 170
8.5.2 Entrant 171
8.5.3 Général 172

8.6 Centre d'appel mini 174
8.6.1 État 174
8.6.2 Lignes 175
8.6.3 Agents 178
8.6.4 Général 179

8.7 Adaptateur TFE 179
8.7.1 Adaptateur TFE 180
8.7.2 Signalisation TFE 181

8.8 Appels d'alarme 184
8.8.1 Appels d'alarme 184

8.9 Système boîte vocale 187

8.9.1 Boîtes vocales . . . 188
8.9.2 État . . . 192
8.9.3 Général . . . 193

Chapitre 9 LAN . . . 196

9.1 Configuration IP . . . 196
9.1.1 Interfaces . . . 196

9.2 VLAN . . . 200
9.2.1 VLAN . . . 200
9.2.2 Configuration du port . . . 201
9.2.3 Administration . . . 202

Chapitre 10 Réseau . . . 203

10.1 Routes . . . 203
10.1.1 Configuration des routes IPv4 . . . 203
10.1.2 Tableau de routage IPv4 . . . 209
10.1.3 Options . . . 210

10.2 NAT . . . 211
10.2.1 Interfaces NAT . . . 211
10.2.2 Configuration NAT . . . 212

10.3 QoS . . . 219
10.3.1 Filtre QoS . . . 219
10.3.2 Classification QoS . . . 222
10.3.3 Interfaces/Directives QoS . . . 225

10.4 Règles d'accès . . . 232
10.4.1 Filtre d'accès . . . 234
10.4.2 Chaînes de règles . . . 237
10.4.3 Affectation des interfaces . . . 239

10.5 Drop-In . . . 240
10.5.1 Groupes Drop-In . . . 240

Chapitre 11 Multicast 243

11.1 Général 245
11.1.1 Général 245

11.2 IGMP 245
11.2.1 IGMP 245
11.2.2 Options 248

11.3 Transférer 249
11.3.1 Transférer 249

Chapitre 12 WAN 251

12.1 Internet + composer 251
12.1.1 PPPoE 254
12.1.2 PPTP 259
12.1.3 RNIS 263
12.1.4 Pool IP 272

12.2 Real Time Jitter Control 273
12.2.1 Interfaces régulées 273

Chapitre 13 VPN 275

13.1 IPSec 275
13.1.1 IPSec-Peers 276
13.1.2 Profils Phase-1 291
13.1.3 Profils Phase-2 299
13.1.4 Profils XAUTH 304
13.1.5 Pool IP 306
13.1.6 Options 306

13.2 L2TP 310
13.2.1 Profils de tunnels 310

13.2.2 Utilisateur . . . 313
13.2.3 Options . . . 318

13.3 PPTP . . . 319
13.3.1 Tunnel PPTP . . . 319
13.3.2 Options . . . 326
13.3.3 Pool IP . . . 327

13.4 GRE . . . 328
13.4.1 Tunnel GRE . . . 328

Chapitre 14 Pare-feu . . . 331

14.1 Directives . . . 333
14.1.1 Règles de filtre . . . 333
14.1.2 QoS . . . 336
14.1.3 Options . . . 337

14.2 Interfaces . . . 338
14.2.1 Groupes . . . 338

14.3 Adresses . . . 339
14.3.1 Liste d'adresses . . . 339
14.3.2 Groupes . . . 340

14.4 Services . . . 340
14.4.1 Liste de services . . . 341
14.4.2 Groupes . . . 343

Chapitre 15 Services locaux . . . 344

15.1 DNS . . . 344
15.1.1 Paramètres globaux . . . 346
15.1.2 Serveur DNS . . . 348
15.1.3 Hôtes statiques . . . 350
15.1.4 Extension de domaine . . . 351
15.1.5 Cache . . . 352

15.1.6 Statistiques . . . 353

15.2 HTTPS . . . 353
15.2.1 Serveur HTTPS . . . 354

15.3 Client DynDNS . . . 354
15.3.1 Mise à jour DynDNS . . . 355
15.3.2 Fournisseur DynDNS . . . 356

15.4 Serveur DHCP . . . 358
15.4.1 Configuration pool d'adresses IP . . . 358
15.4.2 Configuration DHCP . . . 359
15.4.3 Liaison IP/MAC . . . 362
15.4.4 Paramètres DHCP-Relay . . . 363

15.5 Serveur CAPI . . . 364
15.5.1 Utilisateur . . . 364
15.5.2 Options . . . 365

15.6 Scheduling . . . 366
15.6.1 Déclencheur . . . 367
15.6.2 Actions . . . 372
15.6.3 Options . . . 383

15.7 Surveillance . . . 384
15.7.1 Hôtes . . . 384
15.7.2 Interfaces . . . 387
15.7.3 Ping-Generator . . . 388

15.8 UPnP . . . 389
15.8.1 Interfaces . . . 389
15.8.2 Général . . . 390

15.9 Passerelle hotspot . . . 391
15.9.1 Passerelle hotspot . . . 393
15.9.2 Options . . . 396

15.10 Wake-On-LAN . . . 397
15.10.1 Filtre Wake-On-LAN . . . 397

15.10.2 Règles WOL 400
15.10.3 Affectation des interfaces 402

Chapitre 16 Maintenance 403

16.1 Diagnostic 403
16.1.1 Test Ping 403
16.1.2 Test DNS 403
16.1.3 Test Traceroute 403

16.2 Logiciel et configuration 404
16.2.1 Options 404

16.3 Mise à jour de téléphone. 409
16.3.1 Gigaset Téléphone 409
16.3.2 Fichiers du logiciel système 411
16.3.3 Paramètres 412

16.4 Redémarrage 412
16.4.1 Redémarrage système 413

Chapitre 17 Création de rapports externe 414

17.1 Journal système 414
17.1.1 Serveur Syslog 414

17.2 IP-Accounting 416
17.2.1 Interfaces 417
17.2.2 Options 417

17.3 Service de notification 418
17.3.1 Destinataire de la notification 418
17.3.2 Paramètres de notification 420

17.4 SNMP 422
17.4.1 Options SNMP-Trap 422
17.4.2 SNMP-Trap-Hosts 423

Chapitre 18 Monitoring 425

18.1 Information d'état 425
18.1.1 Utilisateur 425
18.1.2 Teams 426

18.2 Journal interne 427
18.2.1 Messages système 427

18.3 IPSec 428
18.3.1 Tunnel IPSec 428
18.3.2 Statistiques IPSec 429

18.4 Interfaces 430
18.4.1 Statistiques 430

18.5 Passerelle hotspot 432
18.5.1 Passerelle hotspot 432

18.6 QoS 432
18.6.1 QoS 433

Index 434

Chapitre 1 Assistants

Le menu **Assistants** fournit des instructions détaillées pour les tâches de configuration de base suivantes :

- **Première étape**
- **Accès Internet**
- **VPN**
- **PBX**

Sélectionnez la tâche correspondante dans le menu de navigation et suivez les instructions et les explications qui s'affichent sur chacune des pages de l'Assistant.

Chapitre 2 Gestion du système

Le menu **Gestion du système** contient des informations et des paramètres système généraux.

Vous disposez d'une vue d'ensemble des états système. Le menu permet également de gérer les paramètres système généraux comme le nom de système, la date / l'heure, les mots de passe et les licences et de configurer les méthodes d'accès et d'authentification.

2.1 État

Lorsque vous vous connectez à l'interface de configuration, la page d'état de l'appareil contenant les principales informations système s'affiche.

Vous disposez d'une vue d'ensemble des données suivantes :

- Etat système
- Activité de l'appareil : Charge des ressources, sessions actives et tunnel
- Etat et configuration de base des interfaces LAN, WAN, RNIS et ADSL.
- Informations sur les modules supplémentaires éventuellement enfichés

Vous pouvez modifier individuellement l'intervalle de mise à jour de la page d'état en saisissant l'intervalle voulu en secondes sous **Intervalle de mise à jour automatique** et en cliquant sur le bouton **Appliquer**.

Attention

Pour **Intervalle de mise à jour automatique**, ne pas saisir de valeur inférieure à *5* secondes, sinon l'écran se rafraîchit à des intervalles trop courts pour pouvoir effectuer d'autres modifications.

Le menu **Gestion du système**->**État** se compose des champs suivants :

Champs du menu informations système

Champ	Valeur
Uptime	Affiche la durée qui s'est écoulée depuis l'appareil a été redémarré.
Date système	Affiche la date et l'heure système actuelles.

Champ	Valeur
Numéro de série	Affiche le numéro de série de l'appareil.
Version BOSS	Affiche la version actuellement chargée du logiciel système.
Ssauvegarde de la configuration sur la carte SD	Indique s'il existe ou non une sauvegarde de la configuration sur la carte SD.
Dernière configuration enregistrée	Affiche le jour, la date et l'heure du dernier enregistrement de la configuration (configuration de mise en route dans le flash).
État Service de nuit	Indique si l'appareil se trouve en service normal (*Arrêt*) ou en service de nuit (*Marche*).

Champs du menu Informations sur les ressources

Champ	Valeur
Utilisation CPU	Affiche la charge de la CPU en pourcentage.
Utilisation de la mémoire vive	Affiche la charge de la mémoire vive en Moctets par rapport à la mémoire vive totale disponible en Moctets. La charge est de plus affichée entre parenthèses en pourcentage.
Carte mémoire	Affiche l'état d'une carte mémoire externe éventuellement enfichée et son volume en Goctets ou en Moctets.
Sessions actives (SIF, RTP, etc...)	Affiche la somme de toutes les sessions SIF, TDRC et charge IP.
Tunnel IPSec actif	Affiche le nombre de liaisons IPSec actuelles par rapport au nombre de liaison IPSec configurée.

Champs du menu Modules

Champ	Valeur
Module DSP	Affiche le type d'un module DSP éventuellement enfiché et les canaux DSP occupés (occupé / disponible). Les licences éventuellement acquises sont également affichées.

Champs du menu Interfaces physiques

Champ	Valeur
Interface - **Information de connexion** - **Lien**	Toutes les interfaces physiques sont listées avec mention des paramètres principaux. Indique également si les interfaces sont raccordées ou actives. Détail des interfaces Ethernet : • Adresse IP • Masque réseau • Non configuré Détail des interfaces RNIS : • Configuré • Non configuré Détail des interfaces xDSL : • Vitesse de la ligne en descente/en montée

Champs du menu Interfaces WAN

Champ	Valeur
Description - **Information de connexion** - **Lien**	Toutes les interfaces WAN sont listées avec mention des paramètres principaux. Indique également si les interfaces sont actives.

2.2 Paramètres globaux

Le menu **Paramètres globaux** permet de gérer les paramètres système de base.

2.2.1 Système

Le menu **Gestion du système**->**Paramètres globaux**->**Système** affiche les données système principales du système.

Le menu **Gestion du système**->**Paramètres globaux**->**Système** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Valeur
Nom du système	Indiquez le nom de système de votre appareil. Il est utilisé également comme nom d'hôte PPP. Une chaîne peut contenir 255 caractères maximum. La valeur par défaut est le type de l'appareil.
Emplacement	Indiquez l'endroit où se trouve votre appareil.
Contact	Saisissez l'interlocuteur compétent. Permet de saisir les adresses mail de l'administrateur système. Une chaîne peut contenir 255 caractères maximum.
Nombre maximal d'entrées de journal Syslog	Saisissez le nombre maximal de messages protocole système qui doivent être enregistrés en interne sur l'appareil. Les valeurs possibles sont comprises entre *0* et *1000*. La valeur par défaut est *50*. Vous pouvez afficher les messages enregistrés **Monitoring**->**Journal interne**.
Niveau maximal de messages des entrées de journal système	Sélectionnez la priorité des messages système à partir de laquelle ils sont journalisés. Seuls les messages de protocole système dont la priorité est supérieure ou égale à celle indiquée sont enregistrés en interne, c'est-à-dire que pour la priorité *Debug*, tous les messages créés sont enregistrés. Valeurs possibles : • *Urgence* : Seuls les messages portant la priorité Urgence sont enregistrés. • *Alarme* : Les messages portant la priorité Urgence et Alarme sont enregistrés. • *Critique* : Les messages portant la priorité Urgence, Alarme et Critique sont enregistrés. • *Erreur* : Les messages portant la priorité Urgence, Alarme, Critique et Erreur sont enregistrés. • *Avertissement !* : Les messages portant la priorité Urgence, Alarme, Critique, Erreur et Avertissement sont enre-

Champ	Valeur
	gistrés. • *Notification* : Les messages portant la priorité Urgence, Alarme, Critique, Erreur, Avertissement et Notification sont enregistrés. • *Informations* (valeur par défaut) : Les messages portant la priorité Urgence, Alarme, Critique, Erreur, Avertissement, Notification et Informations sont enregistrés. • *Debug* : tous les messages sont enregistrés.
Nombre maximal d'entrées de journal Accounting	Saisissez le nombre maximal d'entrées qui peuvent être enregistrées en interne sur l'appareil dans le journal. Les valeurs possibles sont comprises entre *0* et *1000*. La valeur par défaut est *20*.

Transmission à l'abonné occupé

Dans la configuration, on peut définir si la transmission d'un appel vers un abonné occupé est possible ou si pour « Arrêt » le correspondant entend le signal occupé, ce qui termine l'appel. Sinon, le correspondant reste en ligne et il entend la tonalité ou une musique d'attente. Lorsque l'abonné destinataire raccroche le combiné, l'abonné resté en attente entend la tonalité. L'abonné destinataire est appelé et il peut prendre l'appel en attente.

Champs du menu Réglage système

Champ	Valeur
Signalisation de la transmission	Définissez comment s'effectue l'acheminement vers un abonné interne. Valeurs possibles : • *Avec tonalité* (valeur par défaut) : Le correspondant entend la tonalité pendant l'acheminement. • *Avec musique d'attente (Music on Hold, MoH)* : Le correspondant entend une musique d'attente du système pendant l'acheminement.
Transmission à l'abonné occupé	Définissez si l'acheminement vers un abonné occupé est possible. Sélectionnez *Activé* pour activer la fonction.

Champ	Valeur
	La fonction est désactivée par défaut.
Rejet vers un numéro d'appel	Définissez la destination de renvoi des appels entrants, p.ex. en cas d'erreur de numéro. Valeurs possibles : • *Pas de rejet – Sonnerie "occupé"* : Le correspondant entend par défaut la sonnerie occupé et ne peut pas être renvoyé vers un destinataire. • *<Numéro d'appel>* : L'appel entrant est orienté par défaut vers le numéro d'appel sélectionné. La valeur par défaut est le numéro d'appel interne prédéfini *40 (Team global)*.
Coupler les connexions externes	Indiquez si en cas de va-et-vient avec deux correspondants externes, ils doivent être mis en communication une fois que vous avez reposé le combiné. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Réglages du pays

Votre entreprise est une entité internationale qui possède des filiales dans plusieurs pays. Malgré les différences d'architecture des nationaux, vous voulez utiliser le même système dans chaque filiale. Le réglage des variantes par pays permet d'adapter le système aux particularités du réseau national concerné.

Sachant que les exigences posées au système varient en fonction des pays, la fonctionnalité doit être adaptée à un certain nombre de caractéristiques. Les paramètres de base des différentes variante par pays sont enregistrés dans le système.

Champs du menu Réglages du pays

Champ	Valeur
Réglage du pays	Sélectionnez le pays dans lequel le système doit être utilisé. Remarque : Ceci active la langue des textes du menu système des téléphones. Valeurs possibles :

Champ	Valeur
	• *Allemagne* (valeur par défaut) • *Pays-Bas* • *Great Britain* • *België* • *Italia* • *Danmark* • *España* • *Sverige* • *Norge* • *France* • *Portugal* • *Autriche* • *Suisse* • *Česko* • *Slovenija* • *Polska* • *Magyarország* • *Ellada*
Langue d'affichage	Réglez la langue voulue pour le menu système. Le système propose un menu spécial - Menu système - avec des fonctions spécifiques en lien avec le système. L'affichage dans le menu système peut s'effectuer dans différentes langues. Ce réglage est différent de celui des paramètres des téléphones du système proprement dits. Valeurs possibles : • *Deutsch* (valeur par défaut) • *Englisch* • *Italien*
Préfixe international/Indicatif pays	Saisissez le code du pays. Cette entrée est nécessaire si vous voulez générer automatiquement un numéro d'appel international sous **Fournisseur SIP**. Vous composez comme d'habitude l'indicatif national p.

Champ	Valeur
	ex. 05151 909999 et le système compose automatiquement +495151 909999. Si vous n'inscrivez pas le code pays, il peut y a voir une erreur et le système compose le +5151 909999. Sans l'entrée **Créer un numéro d'appel international** et **Préfixe international/Indicatif pays** il faut toujours composer le numéro complet avec l'indicatif du pays pour les fournisseurs SIP. Remarque : Tous les fournisseur SIP ne prennent pas en charge cette configuration.
Préfixe national/Indicatif réseau local	Renseignez le préfixe national ou l'indicatif local du lieu sur lequel le système est installé. Cet indicatif du réseau local est indispensable, sinon le rappel automatique vers l'extérieur n'est pas possible.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres de facturation

Champ	Valeur
Facteur d'unité de tarification	Saisissez le facteur de calcul des coûts de connexion. La valeur par défaut est *0,00*.
Devise	Indiquez la devise, p. ex. *EUR*, (trois caractères au plus). Il s'agit juste d'un nom, qui n'est pas pris en compte pour le calcul du facteur des unités de tarification. Les caractères spéciaux ne sont pas admis.
Information sur les taxes (extension S0/Upn)	Sélectionnez le mode de transmission des informations tarifaires vers le bus interne S0. Valeurs possibles : • *Clavier* : En fonction des pays et du fournisseur, ces informations peuvent être transmises de sorte qu'elles s'affichent directement sur le terminal. • *Fonctionnel* : Les informations tarifaires sont transmises sous forme de code binaire et doivent être décodées par le terminal (EURO ISDN). • *Les deux* (valeur par défaut) : Les deux protocoles sont reconnus.

Champs du menu Mode jour

Champ	Valeur
Rejet global	Sélectionnez la variante d'appel en mode Jour qui s'applique à l'ensemble du système en l'absence de rejet spécifique. La valeur par défaut est *Variante 1*.

Service de nuit

Vous pouvez brancher le système en mode Service de nuit et activer ainsi certaines variantes d'appel pour la signalisation Equipe, la signalisation TFE et les fonctions de rejet.

Il est possible d'élargir la commutation des variantes d'appel via un code ou un calendrier configuré pour le service de nuit. La configuration d'un calendrier pour le service de nuit s'effectue dans le menu **Applications**->**Calendrier**->**Calendrier**->**Nouveau**.

Champs du menu Service de nuit

Champ	Valeur
Signalisation groupée	Sélectionnez la variante d'appel pour la signalisation Equipe en service de nuit.
Signalisation TFE	Sélectionnez la variante d'appel TFE pour la signalisation TFE en service de nuit.
Rejet sur l'annonce	Sélectionnez la variante d'appel pour Rejet sur l'annonce en service de nuit.
Rejet individuel de l'abonné	Sélectionnez la variante d'appel pour Rejet vers numéro direct en service de nuit.
Rejet global	Sélectionnez la variante d'appel pour Rejet général en service de nuit.
Entrée d'alarme	Sélectionnez la variante d'appel pour Alarme en service de nuit.

2.2.2 Mots de passe

La définition des mots de passe fait également partie des paramètres de base.

Note

Tous les appareils **Gigaset** sont fournis avec le même nom d'utilisateur, le même mot de passe et les mêmes PIN. Ils ne sont donc pas protégé contre un accès non autorisé tant que les mots de passe et les PIN n'ont pas été changés.

Lorsque vous vous connectez la première fois à votre terminal, vous être invité à changer le mot de passe. Vous devez modifier le mot de passe Administrateur pour pouvoir configurer votre appareil.

Vous devez impérativement modifier tous les mots de passe et les PIN, afin d'éviter tout accès non autorisé à votre appareil.

Le menu **Gestion du système**->**Paramètres globaux**->**Mots de passe** se compose des champs suivants :

Champs du menu Mot de passe système

Champ	Valeur
Mot de passe de l'administrateur système	Saisissez le mot de passe pour l'utilisateur `admin`. Dans SNMPv3, ce mot de passe est aussi utilisé pour l'authentification (MD5) et le cryptage (DES).
Confirmer le mot de passe de l'administrateur système	Confirmez le mot de passe et le saisissant une nouvelle fois.

PIN1 et PIN2

Différentes fonctions de protection permettent d'éviter une utilisation abusive de votre système. Vous protégez le paramétrage de votre système à l'aide d'un code d'identification de quatre caractères (PIN1, code secret). Vous vous protégez contre tout accès externe (accès distant) à l'aide d'un code d'identification de 6 caractères (PIN2).

Le PIN1 est un code secret de quatre caractères qui permet de protéger les paramètres de l'installation contre tout accès non autorisé. Le PIN2 est un code secret de six caractères qui bloque l'accès au système de tout abonné externe non autorisé. Ces fonctions sont utilisables après avoir saisi un code PIN2 à 6 caractères.

Différents paramètres sont protégés par PIN1. Dans les paramètres de base, PIN1 est réglé sur *`none`*.

Les fonctionnalités suivantes sont protégées par PIN2 :

- Accès distant pour Follow me, surveillance de la pièce

Champs du menu Configuration par téléphone (PIN à quatre chiffres, numérique)

Champ	Valeur
PIN1	Saisissez PIN1. Vous protégez le paramétrage de votre système à l'aide du PIN1 (code secret) de quatre caractères en le configurant via un téléphone.

Champs du menu Accès distant téléphonie (PIN à six chiffres)

Champ	Valeur
Accès distant (p.ex. Follow me, surveillance de la pièce)	Indiquez si l'accès distant au système doit être autorisé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
PIN2	Uniquement si **Accès distant (p.ex. Follow me, surveillance de la pièce)** est activé. Saisissez le **PIN2**. La valeur par défaut est *000000*. Vous vous protégez contre tout accès externe (accès distant) à l'aide du **PIN2** de 6 caractères.

Champs du menu SNMP-Communities

Champ	Valeur
SNMP Read Community	Saisissez le mot de passe pour l'utilisateur `read`.
SNMP Write Community	Saisissez le mot de passe pour l'utilisateur `write`.

Champ du menu Options de mot de passe globales

Champ	Valeur
Afficher les mots de passe et la clé en clair	Indiquez si les mots de passe doivent être affichés en clair. Sélectionnez *Affichage* pour activer la fonction.

Champ	Valeur
	La fonction est désactivée par défaut. Si vous avez activé la fonction, tous les mots de passe et les clés de tous les menus sont affichés et être édités en clair. Les clés IPSec constituent une exception. Elles ne peuvent être saisies qu'en clair. Après avoir cliqué sur **OK** ou après appel du menu, elles sont affichées sous forme d'étoiles.

2.2.3 Date et heure

Le temps du système est nécessaire entre autres pour l'horodatage des messages système ou la saisie des coûts.

Pour la détermination du temps système (temps local) vous disposez des possibilités suivantes :

RNIS/manuel

Le temps système peut être actualisé via RNIS, c'est-à-dire qu'à chaque connexion externe existante, la date et l'heure sont récupérées du RNIS. La date et l'heure peuvent aussi être récupérées manuellement, par ex. si dans RNIS la date et l'heure ne sont pas transmises ou si aucun serveur horaire n'est disponible. L'heure est conservée environ 3 heures après l'arrêt de l'alimentation électrique du système.

Le changement d'heure (heure d'hiver, heure d'été) est automatique. La commutation est indépendante de l'heure du central ou du serveur ntp. L'heure d'été commence le dernier dimanche de mars ; à 2 heures il est 3 heures. Les commutation programmées dans le calendrier ou l'agenda de l'appareil durant cette heure manquante sont effectuées immédiatement après le changement d'heure. L'heure d'hiver commence le dernier dimanche d'octobre ; à 3 heures il est 2 heures. Les commutation programmées dans le calendrier ou l'agenda de l'appareil durant cette heure supplémentaire sont effectuées immédiatement après le changement d'heure.

Serveur horaire

Vous pouvez récupérer l'heure système automatiquement sur différents serveurs horaires. Afin de s'assurer que l'appareil utilise effectivement l'heure voulue, il est préférable de configurer un ou plusieurs serveurs horaires.

Note

Si une méthode de récupération automatique du temps est définie sur un appareil, les valeurs obtenues de cette manière sont prioritaires. Le temps système saisi manuellement est écrasé.

Le menu **Gestion du système**->**Paramètres globaux**->**Date et heure** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Plage horaire	Sélectionnez le fuseau horaire dans lequel l'appareil installé. Il est possible de sélectionner le Universal Time Coordinated (UTC) plus ou moins l'écart en heure ou un lieu prédéfini, p. ex. *Europe/Berlin*.
Heure locale actuelle	Affiche ici la date et l'heure système actuelles. L'entrée ne peut pas être modifiée.

Champs du menu Réglage manuel de l'heure

Champ	Description
Régler la date	Saisissez une nouvelle date. Format : • **Jour** : jj • **Mois** : mm • **Année**: aaaa
Réglage de l'heure	Saisissez une nouvelle heure. Format : • **Heure**: hh • **Minute** : mm

Champs du menu Réglage automatique de l'heure (protocole d'heure)

Champ	Description
Serveur horaire RNIS	Déterminez si l'heure système doit être actualisée via RNIS.

Champ	Description
	Si un serveur horaire est configuré, l'heure est déterminée via RNIS jusqu'à ce que le serveur horaire soit mis à jour avec succès. Pour la période durant laquelle l'heure est déterminée via un serveur horaire, la mise à jour via RNIS est mise hors service. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Premier serveur horaire	Saisissez le premier serveur horaire en indiquant soi son nom de domaine, soit son adresse IP. Sélectionnez en outre le protocole d'interrogation du serveur horaire. Valeurs possibles : • *SNTP* (valeur par défaut) : Ce serveur utilise le Simple Network Time Protocol via le port UDP 123. • *Time Service / UDP* : ce serveur utilise le service horaire via le port UDP 37. • *Time Service / TCP* : ce serveur utilise le service horaire via le port TCP 37. • *aucun* : ce serveur horaire n'est temporairement pas utilisé pour l'interrogation horaire. A la livraison, le serveur *ntp1.sda.t-online.de* est configuré par défaut.
Deuxième serveur horaire	Saisissez le deuxième serveur horaire en indiquant soi son nom de domaine, soit son adresse IP. Sélectionnez en outre le protocole d'interrogation du serveur horaire. Valeurs possibles : • *SNTP* (valeur par défaut) : Ce serveur utilise le Simple Network Time Protocol via le port UDP 123. • *Time Service / UDP* : ce serveur utilise le service horaire via le port UDP 37. • *Time Service / TCP* : ce serveur utilise le service horaire

Champ	Description
	via le port TCP 37. • *aucun* : ce serveur horaire n'est temporairement pas utilisé pour l'interrogation horaire. A la livraison, le serveur *ntp1.sul.t-online.de* est configuré par défaut.
Troisième serveur horaire	Saisissez le troisième serveur horaire en indiquant soi son nom de domaine, soit son adresse IP. Sélectionnez en outre le protocole d'interrogation du serveur horaire. Valeurs possibles : • *SNTP* (valeur par défaut) : Ce serveur utilise le Simple Network Time Protocol via le port UDP 123. • *Time Service / UDP* : ce serveur utilise le service horaire via le port UDP 37. • *Time Service / TCP* : ce serveur utilise le service horaire via le port TCP 37. • *aucun* : ce serveur horaire n'est temporairement pas utilisé pour l'interrogation horaire.
Intervalle de mise à jour de l'heure	Saisissez le délai de mise à jour automatique de l'heure, en minutes. La valeur par défaut est *1440*.
Directive de mise à jour de l'heure	Renseignez le délai pour accéder à nouveau au serveur horaire après un échec de mise à jour de l'heure. Valeurs possibles : • *Normal* (valeur par défaut) : le serveur est accédé après 1, 2, 4, 8 et 16 minutes. • *Agressif* : Pendant 10 minutes, le serveur horaire est accédé après secondes et ensuite toutes les 10 secondes. • *Sans fin* : Le serveur horaire est accédé sans limite de temps après 1, 2, 4, 8 secondes et ensuite toutes les 10 secondes. En cas d'utilisation de certificats pour le cryptage du flux de

Champ	Description
	données dans un VPN, est il indispensable de bien régler l'heure sur l'appareil. Pour vous en assurez, choisissez comme **Directive de mise à jour de l'heure** la valeur *Sans fin*.
Système en tant que serveur horaire	Indiquez si le serveur horaire interne doit être utilisé. Sélectionnez *Activé* pour activer la fonction. Lorsqu'un client demande l'heure, l'heure système lui est renvoyée. Elle est indiquée en GMT sans décalage. La fonction est activée par défaut. Les demandes d'heure du client dans le LAN sont renseignées.

2.2.4 Horloge

Dans le menu **Horloge**, vous pouvez configurer les horaires de commutation par défaut de certaines fonctionnalités système.

Le menu **Gestion du système**->**Paramètres globaux**->**Horloge** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Transfert des appels (CFNR)	Saisissez ici le temps à l'issue duquel une **Transfert des appels (CFNR)** doit être exécutée. Les valeurs possibles sont comprises entre *1* et *99*. La valeur par défaut est *15*.
Appel direct	Indiquez au bout de combien de temps après avoir décroché le combiné le numéro sélectionné doit être configuré. Vous souhaitez configurer un téléphone permettant d'établir une communication vers un numéro d'appel défini sans devoir composer le numéro d'appel en question (p. ex. un téléphone d'appel d'urgence). Vous êtes en déplacement. Pourtant, il y a quelqu'un à la maison que vous devez pouvoir joindre rapidement et facilement en cas de besoin (p. ex. les enfants ou les grands-parents). Si vous avez configuré la fonction « Appel direct » pour un ou plusieurs téléphones, il vous suffit de décrocher le combiné du téléphone en question. Une fois le délai

Champ	Description
	configuré écoulé, en l'absence d'une autre saisie, le système sélectionne automatiquement le numéro d'appel direct défini. Si vous n'effectuez pas de sélection dans le délai imparti après avoir décroché le téléphone, la numérotation automatique est effectuée. Les valeurs possibles sont comprises entre *1* et *30*. La valeur par défaut est *5*.
Connexion externe TFE	Si un appel TFE est demandé sur un téléphone externe, vous pouvez régler le délai après lequel la communication est interrompue. Valeurs possibles : • *Sans fin* • *60 secondes* • *120 secondes* • *180 secondes* (valeur par défaut) • *240 secondes* • *300 secondes*

Champs du menu Paramètres étendus

Champ	Valeur
Transfert de communication sans annonce (UbA)	Indiquez le délai après lequel un abonné non disponible peut être appelé à nouveau ou recevoir un signal d'appel en attente pour une communication entrante. Vous avez transféré un correspondant à un autre abonnée par acheminement ou transmission. Cet abonné n'est pas accessible ou est occupé. Mais vous ne voulez pas que l'abonné raccroche ou que l'appel soit rejeté par le système après un temps donné. Vous pouvez pour cela définir un rappel automatique sur votre téléphone. Pour les communications qui sont transférées sans annonce (bascules de type spécial, UbA) un rappel ou un signal d'appel en attente (si une autre communication est en cours) intervient après le temps donné ici. Les valeurs possibles sont comprises entre *10* et *179*.

Champ	Valeur
	La valeur par défaut est *30*.
Transmission à l'abonné occupé	Saisissez ici le temps à l'issue duquel un abonné en attente est mis à nouveau en relation avec le central. Le central veut transmettre un appel à un collaborateur donné. Il est déjà en communication à ce moment-là. L'appel est mis dans la file d'attente de l'abonné. Si l'appel n'est pas accepté pendant la période de temps définie ici, il bascule à nouveau vers le central. Les valeurs possibles sont comprises entre *10* et *600*. La valeur par défaut est *30*.
Questions ouvertes	Indiquez le délai après lequel appel en attente (parcage) est terminé et l'abonné peut être appelé à nouveau ou recevoir un signal d'appel en attente. Vous êtes en communication et vous voulez le transférer à un collègue. Mais vous ne savez pas où se trouve le collègue au moment donné. L'option **Questions ouvertes** met le correspondant sur la file d'attente du système. Vous pouvez alors lancer une annonce à partir de votre téléphone pour signaler à votre collègue qu'il a une communication en attente. En saisissant le code correspondant au parcage, le collègue peut prendre la communication sur n'importe quel téléphone. Si un appel en attente n'est pas accepté par un abonné dans le temps défini ici, l'abonné qui a transféré l'appel est rappelé automatiquement ou reçoit un signal d'appel en attente. Les valeurs possibles sont comprises entre *10* et *600*. La valeur par défaut est *30*.

2.2.5 Licences système

Ce chapitre montre les licences logicielles activées à la livraison.

Les options d'édition, de création et de restauration ne sont en règle générale pas nécessaires.

Valeurs possibles pour État

Licence	Signification
OK	Le sous-système est activé.
Pas OK	Le sous-système n'est pas activé.
Non pris en charge	Vous avez indiqué une licence pour un sous-système que votre système ne prend pas en charge.

De plus, l'**ID licence système** est affiché au dessus de la liste.

2.2.5.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour saisir d'autres licences.

Le menu **Gestion du système**->**Paramètres globaux**->**Licences système**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Valeur
Numéro de série de la licence	Renseignez le numéro de licence qui vous a été fourni à l'achat de la licence.
Clé de licence	Saisissez la clé de licence que vous avez reçu par mail.

2.3 Codes

Dans vos activités quotidiennes, vous avez utilisé pour certaines fonctionnalités des codes que vous souhaitez continuer d'utiliser dans le nouveau système. Mais dans les paramètres de base, d'autres codes ont été réglés pour cette fonctionnalité. Pas de problème : pour chaque fonctionnalité, vous pouvez ajouter des codes individuellement. Vous êtes donc en mesure de conserver les codes dont vous aviez l'habitude pour cette fonctionnalité.

2.3.1 Codes modifiables

Dans le menu **Codes modifiables**, vous configurez le plan de codes du système.

Il est possible de régler individuellement les codes de certaines fonctionnalités dans la configuration du système. Dans ce cas, le code prédéfini est complété par un numéro provenant du plan interne des numéros d'appel du système. Pour les fonctionnalités **Parcage** et **Groupage**, il est possible d'attribuer plusieurs codes. La commande de la fonctionnalité

avec des codes modifiés s'effectue comme indiqué dans le descriptif de la fonction. Vous pouvez utiliser au choix le code modifié (numéro d'appel interne) ou le code décrit dans le mode d'emploi (sauf les indicatifs).

Le menu **Gestion du système**->**Codes**->**Codes modifiables** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Indicatif	Sélectionnez l'indicatif. Valeurs possibles : • *aucun* • *0* (valeur par défaut) • *6* • *7* • *8* • *9*
Groupe Pick-Up	Indiquez le nouveau code de la fonctionnalité **Pick-Up (groupe)**.
Pick-Up ciblé	Indiquez le nouveau code de la fonctionnalité **Pick-Up (abonné interne)**.
Attribution des numéros de projet	Indiquez le nouveau code de la fonctionnalité **Attribution des numéros de projet**.
Numérotation abrégée	Indiquez le nouveau code de la fonctionnalité **Numérotation abrégée**.
Sélection manuelle du groupage	Indiquez les nouveaux codes de la fonctionnalité **Sélection manuelle du groupage**. Créez pour cela une sélection de groupage en cliquant sur **Ajouter**, sélectionnez le groupage et saisissez le code correspondant à ce groupage.
Questions ouvertes	Indiquez les nouveaux codes de la fonctionnalité **Questions ouvertes**.

Champ	Description
	Créez pour cela une file d'attente en cliquant sur **Ajouter** dans laquelle l'appel est conservé et saisissez le code correspondant à cette file d'attente. Vous pouvez créer au plus 10 entrées.

2.4 Mode Interface / groupes Bridge

Dans ce menu, vous définissez le mode de fonctionnement des interfaces de l'appareil.

Routage et Bridging

Le Bridging permet de raccorder des réseaux semblables. Au contraire des routeurs, les ponts interviennent en couche 2 (couche de protection) du modèle OSI, ils dépendent de protocoles plus évolués et transmettent les paquets de données en fonction des adresses MAC. La transmission des données est transparente, c'est-à-dire que les paquets de données ne sont pas interprétés.

Le routage permet de raccorder des réseaux différents sur la couche 3 (couche réseau) du modèle OSI et de transférer les informations d'un réseau vers un autre (routage).

Conventions pour les noms de port/d'interface

Si l'appareil dispose d'un port radio, il prend le nom d'interface WLAN. S'il existe plusieurs modules radio, les noms des ports radio dans l'interface utilisateur de l'appareil sont composés comme suit :

(a) WLAN

(b) Numéro du port physique (1 ou 2)

Exemple : *WLAN1*

Le nom du port Ethernet se compose des éléments suivants :

(a) ETH

(b) Numéro du port

Exemple : *ETH1*

Le nom de l'interface raccordée à un port Ethernet se compose des éléments suivants :

(a) Abréviation du type d'interface, *en* signifiant Ethernet

(b) Numéro du port Ethernet

(c) Numéro de l'interface

Exemple : *en1-0* (première interface sur le premier port Ethernet)

Le nom du port groupe Bridge se compose des éléments suivants :

(a) Abréviation du type d'interface, *br* signifiant groupe Bridge

(b) Numéro du groupe Bridge

Exemple : *br0* (premier Groupe Bridge)

Le nom du réseau sans fil (VSS) se compose des éléments suivants :

(a) Abréviation du type d'interface, *vss* signifiant réseau sans fil

(b) Numéro du module radio

(c) Numéro de l'interface

Exemple : *vss1-0* (premier réseau sans fil sur le premier module radio)

Le nom du lien WDS ou du lien Bridge se compose des éléments suivants :

(a) Abréviation du type d'interface

(b) Numéro du module radio sur lequel le WDS-Link ou le Bridge-Link est configuré.

(c) Numéro du WDS-Link ou le Bridge-Link

Exemple : *vds1-0* (premier WDS-Link ou Bridge-Link sur le premier module radio)

Le nom du lien client se compose des éléments suivants :

(a) Abréviation du type d'interface

(b) Numéro du module radio sur lequel le lien client est configuré.

(c) Numéro du lien client

Exemple : *sta1-0* (premier réseau lien client sur le premier module radio)

Le nom de l'interface virtuelle raccordée à un port Ethernet se compose des éléments suivants :

(a) Abréviation du type d'interface

(b) Numéro du port Ethernet

(c) Numéro de l'interface raccordée au port Ethernet

(d) Numéro de l'interface virtuelle

Exemple : *en1-0-1* (première interface virtuelle basée sur la première interface du premier port Ethernet)

2.4.1 Interfaces

Pour chaque interface, vous définissez séparément si elle doit fonctionner en mode routage ou en mode pont.

Si vous activez le mode pont, vous pouvez choisir entre des groupes Bridge existants ou en créer un nouveau.

Par défaut, toutes les interfaces existantes sont en mode routage. Si vous sélectionnez l'option *Nouveau groupe Bridge* pour **Mode / Groupe Bridge**, un groupe Bridge est créé automatiquement, soit *br0*, *br1* etc. et l'interface fonctionne en mode pont.

Le menu **Gestion du système**->**Mode Interface / groupes Bridge**->**Interfaces** se compose des champs suivants :

Champs du menu Interfaces

Champ	Description
Description de l'interface	Permet d'afficher le nom de l'interface.
Mode / Groupe Bridge	Indiquez si vous voulez utiliser l'interface en *Mode de routage*, l'affecter à un groupe Bridge existant (*br0*, *br1* etc.) ou à un nouveau groupe Bridge (*Nouveau groupe Bridge*). Si vous sélectionnez *Nouveau groupe Bridge*, un nouveau groupe Bridge est créé automatiquement lorsque vous cliquez sur le bouton **OK**.
Interface de configuration	Sélectionnez l'interface sur laquelle la configuration est exécutée. Valeurs possibles : • *Sélectionner* (valeur par défaut) : Paramètres à la livraison. L'interface de configuration doit être sélectionnée dans les autres options. • *Ignorer* : Aucune interface de configuration n'est définie. • *<Nom de l'interface>* : Définissez l'interface à utiliser pour la configuration. Si cette interface fait partie d'un groupe Bridge, elle prend son adresse IP si elle est sortie du groupe Bridge.

2.4.1.1 Ajouter

Ajouter

Choisissez le bouton **Ajouter** pour éditer le mode des interfaces PPP.

Le menu **Gestion du système**->**Mode Interface / groupes Bridge**->**Interfaces**->**Ajouter** se compose des champs suivants :

Champs du menu Interfaces

Champ	Description
Interface	Sélectionnez l'interface dont vous voulez modifier le mode.

2.5 Accès administratif

Dans ce menu, vous pouvez créer l'accès administratif à l'appareil.

2.5.1 Accès

Le menu **Gestion du système**->**Accès administratif**->**Accès** affiche la liste de toutes les interfaces conformes IP.

Pour une interface Ethernet, les paramètres d'accès *Telnet*, *SSH*, *HTTP*, *HTTPS*, *Ping*, *SNMP* et pour les interfaces RNIS le paramètre *Identifiant RNIS* peuvent être sélectionnés.

Uniquement pour les appareils **hybird** Vous pouvez également activer l'appareil pour les travaux de maintenance via le service client bintec elmeg. Activez pour cela en fonction du service demandé l'option **Service Login (ISDN Web-Access)** ou **Service Call Ticket (SSH Web-Access)** et choisissez le bouton **OK**. Suivez les instructions du service client bintec elmeg.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Restaurer les paramètres de base	Une fois seulement que les modifications de la configuration de l'accès administratif sont terminées, les règles d'accès sont créées et activées. Le symbole vous permet de restaurer

Champ	Description
	les paramètres par défaut.

2.5.1.1 Ajouter

Choisissez **Ajouter** pour configurer l'accès administratif d'autres interfaces.

Le menu **Gestion du système**->**Accès administratif**->**Accès**->**Ajouter** se compose des champs suivants :

Champs du menu Accès

Champ	Description
Interface	Sélectionnez l'interface pour laquelle l'accès administratif doit être configuré.

2.5.2 SSH

Votre appareil propose un accès crypté vers le shell. Vous pouvez activer ou désactiver cet accès dans le menu **Gestion du système**->**Accès administratif**->**SSH** (**Activé**, valeur par défaut). De plus, vous pouvez accéder aux options vers la configuration de la connexion SSH.

Pour accéder au Daemon SSH, il faut une application client SSH, p. ex. PuTTY.

Si vous voulez utiliser SSH Login avec le client PuTTY, vous devez tenir compte de certaines particularités de la configuration. Nous avons créée une rubrique FAQ à cet effet. Elle se trouve dans la zone Services/Assistance sur *www.bintec-elmeg.com* .

Pour atteindre le shell de l'appareil via un client SSH, assurez-vous que les paramètres SSH Daemon et SSH Client sont identiques.

Note

Si la connexion SSH n'est pas possible après la configuration, redémarrez l'appareil pour initier le daemon SSH correctement.

Le menu **Gestion du système**->**Accès administratif**->**SSH** se compose des champs suivants :

Champs du menu Paramètres SSH (Secure Shell)

Champ	Valeur
Service SSH actif	Indiquez si le daemon SSH doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Port SSH	Vous pouvez saisir ici le port via lequel la connexion SSH doit être établie. La valeur par défaut est *22*.
Nombre maximal de connexions simultanées	Saisissez le nombre maximal de connexions SSH actives simultanément. La valeur par défaut est *1*.

Champs du menu Paramètres d'authentification et de cryptage

Champ	Valeur
Algorithmes d'encryptage	Sélectionnez les algorithmes devant servir au cryptage de la connexion SSH. Options possibles : • *3DES* • *Blowfish* • *AES-128* • *AES-256* Par défaut, les options *3DES*, *Blowfish* et *AES-128* sont activées.
Algorithmes de hachage	Sélectionnez les algorithmes devant servir à l'authentification des messages de la connexion SSH. Options possibles : • *MD5* • *SHA-1* • *RipeMD 160* Par défaut, les options *MD5*, *SHA-1* et *RipeMD 160* sont activées.

Champs du menu Etat de la clé

Champ	Valeur
Etat de la clé RSA	Affiche l'état de la clé RSA. Si aucune clé RSA n'a encore été générée, le message *Non généré* s'affiche en rouge avec un lien *Générer*. Cliquer sur le lien lance le processus de génération et met à jour l'affichage. L'état *Génération en cours* s'affiche alors en vert. Une fois la génération terminée, l'état passe de *Génération en cours* à *Généré*. Si une erreur se produit au cours de la génération, le message *Non généré* s'affiche à nouveau avec le lien *Générer*. Vous pouvez recommencer la génération. Si l'état est *Inconnu*, la génération d'une clé est impossible, p. ex. parce que la mémoire FlashROM est insuffisante.
Etat de la clé DSA	Affiche l'état de la clé DSA. Si aucune clé DSA n'a encore été générée, le message *Non généré* s'affiche en rouge avec un lien *Générer*. Cliquer sur le lien lance le processus de génération et met à jour l'affichage. L'état *Génération en cours* s'affiche alors en vert. Une fois la génération terminée, l'état passe de *Génération en cours* à *Généré*. Si une erreur se produit au cours de la génération, le message *Non généré* s'affiche à nouveau avec le lien *Générer*. Vous pouvez recommencer la génération. Si l'état est *Inconnu*, la génération d'une clé est impossible, p. ex. parce que la mémoire FlashROM est insuffisante.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Valeur
Temps de tolérance à la connexion	Saisissez le temps (en secondes) disponible pour établir la connexion. Si un client ne peut pas être authentifié avec succès durant cette période, la connexion est interrompue. La valeur par défaut est *600* secondes.
Compression	Indiquez s'il faut utiliser la compression des données.

Champ	Valeur
	Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
TCP-Keepalives	Indiquez si l'appareil doit envoyer des paquets Keepalive. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Niveau de journalisation	Sélectionnez le niveau Syslog pour les messages du journal système générés par le daemon SSH. Sont disponibles : • *Informations* (valeur par défaut) : Sont affichées, les erreurs graves, les erreurs simples du daemon SSH et les informations. • *Fatal* : Seules les erreurs graves du deamon SSH sont affichées. • *Erreur* : Sont affichées, les erreurs graves et les erreurs simples du daemon SSH. • *Debug* : tous les messages sont enregistrés.

2.5.3 SNMP

SNMP (Simple Network Management Protocol) est un protocole réseau servant à contrôler et à commander les éléments du réseau (p. ex. routeur, serveur, commutateurs, imprimantes, ordinateurs, etc.) à partir d'un poste central. SNMP régule la communication entre les appareils contrôlés et le poste de surveillance. Le protocole décrit la structure des paquets de données qui peuvent être envoyées et le déroulement de la communication.

Les objets de données qui peuvent être interrogés via SNMP sont structurés en tables et variables et définis dans la MIB (Management Information Base). Elle contient les variables de configuration et d'état de l'appareil.

SNMP permet de remplir les tâches de gestion de réseau suivantes :

- Surveillance des composants réseau
- Pilotage et configuration à distance des composants réseau
- Détection et notification des erreurs

Dans ce menu, vous configurez l'utilisation de SNMP.

Le menu **Gestion du système**->**Accès administratif**->**SNMP** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Valeur
Version SNMP	Indiquez la version SNMP que l'appareil doit utiliser pour les accès SNMP externes. Valeurs possibles : • *v1* : SNMP version 1 • *v2c*: Community-Based SNMP-Version 2 • *v3* : SNMP version 3 Par défaut, les options *v1*, *v2c* et *v3* sont activées. Si aucune option n'est sélectionnée, la fonction est désactivée.
Port SNMP-Listes-UDP	Affiche le port UDP (*161*) qui accepte les requêtes SNMP sur l'appareil. La valeur ne peut pas être modifiée.

Tuyau

Si le gestionnaire SNMP prend en charge SNMPv3, préférez cette version car les anciennes versions transmettent les données sans les crypter.

2.6 Authentification distante

Ce menu contient les paramètres d'authentification de l'utilisateur.

2.6.1 RADIUS

RADIUS (Remote Authentication Dial In User Service) est un service qui permet d'échanger des informations d'authentification et de configuration entre l'appareil et un serveur RADIUS. Le serveur RADIUS gère une base de données contenant des informations sur l'authentification des utilisateurs, la configuration et la saisie statistique des données de connexion.

RADIUS peut être utilisé pour effectuer les tâches suivantes :

- Authentification
- Saisie des coûts
- Echange des données de configuration

Dans une connexion entrante, l'appareil envoie une requête au serveur RADIUS avec le nom d'utilisateur et le mot de passe et le serveur consulte sa base de données. Si l'utilisateur est trouvé et peut être authentifié, le serveur RADIUS envoie une confirmation à l'appareil. Cette confirmation contient également des paramètres (attributs RADIUS) que l'appareil utilise comme paramètres de connexion WAN.

Si le serveur RADIUS est utilisé pour saisir les coûts, l'appareil envoie un message Accounting au début de la connexion et un message à la fin de la connexion. Ces messages de début et de fin contiennent des données statistiques sur la connexion (adresse IP, nom de l'utilisateur, débit, coûts).

Paquets RADIUS

Les types de paquets suivants sont envoyés entre le serveur RADIUS et votre appareil (client) :

Types de paquets

Champ	Valeur
ACCESS_REQUEST	Client -> Serveur Lorsque l'appareil reçoit une demande de connexion, le serveur RADIUS est interrogé si l'appareil ne trouve pas de partenaire de communication correspondant.
ACCESS_ACCEPT	Serveur -> Client Une fois que le serveur RADIUS a authentifié les informations contenues dans ACCESS_REQUEST, il retourne ACCESS_ACCEPT vers l'appareil avec les paramètres à utiliser pour l'établissement de la connexion.
ACCESS_REJECT	Serveur -> Client Si les informations contenues dans ACCESS_REQUEST ne correspondent pas à celles de la base de données utilisateur du serveur RADIUS, il retourne ACCESS_REJECT pour refuser la connexion.

Champ	Valeur
ACCOUNTING_START	Client -> Serveur Si un serveur RADIUS est utilisé pour saisir les coûts, l'appareil envoie un message Accounting au début de chaque connexion au serveur RADIUS.
ACCOUNTING_STOP	Client -> Serveur Si un serveur RADIUS est utilisé pour saisir les coûts, l'appareil envoie un message Accounting à la fin de chaque connexion au serveur RADIUS.

Le menu **Gestion du système**->**Authentification distante**->**RADIUS** affiche une liste de tous les serveurs RADIUS saisis.

2.6.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour saisir d'autres serveurs RADIUS.

Le menu **Gestion du système**->**Authentification distante**->**RADIUS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Valeur
Type d'authentification	Sélectionnez le mode d'utilisation du serveur RADIUS. Valeurs possibles : • *Authentification PPP* (valeur par défaut, uniquement pour connexions PPP) : Le serveur RADIUS est utilisé pour réguler l'accès à un réseau. • *Accounting* (uniquement pour connexions PPP) : Le serveur RADIUS est utilisé pour la saisie des données statistiques de connexion. • *Authentification de l'identifiant* : Le serveur RADIUS est utilisé pour contrôler l'accès de votre appareil au shell SNMP. • *Authentification IPSec* : Le serveur RADIUS est utilisé pour transmettre des données de configuration pour les peer IPSec.

Champ	Valeur
	• *WLAN (802.1x)* : Le serveur RADIUS est utilisé pour réguler l'accès à un réseau sans fil. • *XAUTH* : Le serveur RADIUS est utilisé pour authentifier les peer IPSec pour XAuth.
Mode de l'exploitant	Uniquement pour **Type d'authentification** = *Accounting* Sélectionnez dans les applications Hotspot le mode défini par le fournisseur. Dans les applications standard, conservez la valeur *Par défaut*. Valeurs possibles pour les applications Hotspot : • *France Telecom* : Pour les applications Hotspot de France Telecom. • *Serveur bintec HotSpot* : Pour applications Hotspot.
Adresse IP du serveur	Saisissez l'adresse IP du serveur RADIUS.
Mot de passe RADIUS	Saisissez le mot de passe conjoint pour la communication entre le serveur RADIUS et votre appareil.
Mot de passe utilisateur par défaut	Certains serveurs RADIUS ont besoin d'un mot de passe utilisateur pour chaque requête RADIUS. Saisissez de ce fait le mot de passe que votre appareil envoie par défaut au serveur RADIUS dans les requêtes de route Dialout.
Priorité	Si plusieurs serveurs RADIUS veulent créer des entrées, le serveur portant la priorité la plus haute est utilisé en premier. Si ce serveur ne répond pas, le serveur de priorité la plus basse suivante est utilisé, etc. Valeurs possibles comprises entre *0* (priorité la plus haute) et *7* (priorité la plus basse). La valeur par défaut est *0*. Voir aussi **Directive** dans les paramètres élargis.
Entrée active	Indiquez s'il faut utiliser le serveur RADIUS configuré dans cette entrée. Sélectionnez *Activé* pour activer la fonction.

Champ	Valeur
	La fonction est activée par défaut.
Description du groupe	Définissez une nouvelle description de groupe RADIUS ou attribuez à la nouvelle entrée RADIUS un groupe déjà défini. Les serveurs RADIUS configurés d'un groupe sont interrogés en fonction de la **Priorité** et de la **Directive**. Valeurs possibles : • *Nouveau* (valeur par défaut) : Saisissez une nouvelle description de groupe dans la zone de texte. • *Groupe par défaut 0* : Choisissez cette entrée pour des applications spéciales comme la configuration des serveurs Hotspot. • *<Nom de groupe>* : Sélectionnez sur la liste un groupe déjà défini.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Valeur
Directive	Indiquez comment l'appareil doit réagit quand il reçoit une réponse négative à une demande. Valeurs possibles : • *Obligatoire* (valeur par défaut) : Réponse négative à une demande acceptée. • *Non obligatoire* : Réponse négative à une demande non acceptée. Le serveur RADIUS suivant est interrogé jusqu'à ce que l'appareil reçoive une réponse positive d'un serveur configuré.
Port UDP	Saisissez le port UDP à utiliser pour les données RADIUS. Conformément à RFC 2138, les ports standard 1812 sont prévus pour l'authentification (1645 dans les RFC plus anciens) et 1813 pour la saisie des coûts (1646 dans les RFC plus anciens). Consultez la documentation du serveur RADIUS pour connaître le port à utiliser. La valeur par défaut est *1812*.

Champ	Valeur
Server Timeout	Indiquez le temps d'attente maximal entre ACCESS_REQUEST et la réponse, en millisecondes. Une fois ce temps écoulé, la demande est renouvelée conformément à la valeur du champ **Répétitions** ou le serveur RADIUS configuré suivant est interrogé. Les valeurs possibles sont des nombres entiers compris entre *50* et *50000*. La valeur par défaut est *1000* (1 seconde).
Contrôle d'accessibilité	Choisissez une vérification de l'accessibilité du serveur RADIUS dans l'**État** *Inactif*. Un contrôle (Alive-check) est exécuté (toutes les 20 secondes) en envoyant un ACCESS_REQUEST à l'adresse IP du serveur RADIUS. Lorsqu'il est à nouveau accessible, l'**État** repasse sur *actif*. Si le serveur RADIUS est accessible uniquement via une ligne commutée, des coûts imprévus sont possibles si le serveur est *inactif* pendant un certain temps. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Répétitions	Indiquez le nombre de répétitions lorsque la demande ne reçoit pas de réponse. En l'absence de réponse après ces tentatives répétées, l'**État** passe sur *inactif*. Pour **Contrôle d'accessibilité** = *Activé*, l'appareil essaie d'accéder au serveur toutes les 20 secondes. Lorsque le serveur répond, l'**État** repasse sur *actif*. Les valeurs possibles sont des nombres entiers compris entre *0* et *10*. La valeur par défaut est *1*. Pour éviter que l'**État** passe sur *inactif*, mettez cette valeur à *0*.
RADIUS-Dialout	Uniquement pour **Type d'authentification** = *Authentification PPP* et *Authentification IPSec* Indiquez si l'appareil demande des routes dialout au serveur RADIUS. De cette manière, il est possible de créer automatiquement des interfaces temporaires et l'appareil peut initier

Champ	Valeur
	des connexions qui ne sont pas configurées. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Si une fonction est active, vous pouvez saisir les options suivantes : • *Intervalle de rechargement* : Indiquez la durée en secondes entre les intervalles de mise à jour. La valeur par défaut est *0*, c'est-à-dire qu'il n'y a pas de rechargement automatique.

2.6.2 TACACS+

TACACS+ permet de commander l'accès de l'appareil aux serveurs d'accès réseau (NAS) et autres composants réseau via un ou plusieurs serveurs centraux.

TACACS+ est, comme RADIUS, un protocole AAA et propose des services d'authentification, d'autorisation et de facturation (la saisie des coûts TACACS+ n'est actuellement pas prise en charge par les appareils **Gigaset**).

Les fonctions TACACS+ suivantes sot disponibles sur votre appareil :

- Authentification pour Login Shell
- Autorisation de commande sur le shell (p. ex. telnet, show)

TACACS+ utilise le port TCP 49 et établit une liaison protégée et cryptée.

Le menu **Gestion du système**->**Authentification distante**->**TACACS+** affiche une liste de tous les serveurs TACACS+ saisis.

2.6.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour saisir d'autres serveurs TACACS+.

Le menu **Gestion du système**->**Authentification distante**->**TACACS+** ->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Type d'authentification	Affiche les fonctions TACACS+ à utiliser. La valeur ne peut pas être modifiée. Valeurs possibles : • *Authentification de l'identifiant* : Vous pouvez indiquer ici s'il faut utiliser le serveur TACACS+ actuel pour l'authentification Login.
Adresse IP du serveur	Saisissez l'adresse IP du serveur TACACS+ à interroger pour l'authentification Login.
Mot de passe TACACS+	Saisissez le mot de passe utilisé pour authentifier et (le cas échéant) crypter l'échange de données entre le serveur TACACS+ et le serveur d'accès (votre appareil). L'entrée doit contenir 32 caractères maximum.
Priorité	Attribuez une priorité au serveur TACACS+. Le serveur dont la valeur est la plus basse est le premier qui est utilisé pour l'authentification Login TACACS+. S'il ne donne pas de réponse ou si l'accès est refusé (uniquement pour **Directive** = *Non obligatoire*), l'entrée avec la priorité la plus basse suivante est utilisée. Les valeurs disponibles sont comprises entre *0* et *9*, la valeur par défaut est *0*.
Entrée active	Indiquez si ce serveur doit être utilisé pour l'authentification Login. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Directive	Sélectionnez l'interprétation de la réponse TACACS+. Valeurs possibles : • *Non obligatoire* (valeur par défaut) : Les serveurs TA-

Champ	Description
	CACS+ sont interrogés en fonction de leur priorité (voir **Priorité**), jusqu'à obtention d'une réponse positive ou d'une réponse négative provenant d'un serveur en charge de l'autorisation. • *Obligatoire* : Réponse négative à une demande acceptée, aucun autre serveur TACACS+ n'est interrogé. La gestion des utilisateurs interne à l'appareil n'est pas désactivée par TACACS+. Elle est vérifiée une fois que tous les serveurs TACACS+ ont été interrogés.
Port TCP	Affiche le port TCP standard (*49*) utilisé pour le protocole TACACS+. La valeur ne peut pas être modifiée.
Timeout	Indiquez le temps en secondes pendant lequel le NAS doit attendre une réponse de TACACS+. Si pendant ce temps d'attente aucune réponse n'est reçue, le serveur TACACS+ configuré ensuite est interrogé (uniquement pour **Directive** = *Non obligatoire*) et le serveur actuel passe à l'état *bloqué*. Les valeurs possibles sont comprises entre *1* et *60*, la valeur par défaut est *3*.
Temps de blocage	Indiquez le temps en secondes pendant lequel le serveur actuel doit rester à l'état bloqué. Après la fin du blocage, le serveur passe à l'état indiqué dans le champ **Entrée active**. Les valeurs possibles sont comprises entre *0* et *3600*, la valeur par défaut est *60*. La valeur *0* signifie que le serveur ne passe jamais à l'état *bloqué* et que les autres serveurs ne sont jamais interrogés.
Cryptage	Indiquez si l'échange des données entre le serveur TACACS+ et NAS doit être crypté avec MD5. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut. Si la fonction n'est pas active, les paquets et toutes les informations qui s'y rapportent sont transmis sans cryptage. La

Champ	Description
	transmission non cryptée n'est pas recommandée comme un paramètre par défaut, mais uniquement à des fins de débogage.

2.6.3 Options

Sur la base des paramètres possibles ici, l'appareil exécute une négociation d'authentification pour les appels entrants s'il ne peut pas identifier le Calling Party Number (p. ex. parce que le poste correspondant ne signale pas de Calling Party Number). Si les données reçues à l'aide du protocole d'authentification exécuté (mot de passe , ID partenaire PPP) correspondent à celles du poste correspondant ou d'un utilisateur RADIUS, l'appareil accepte l'appel entrant.

Le menu **Gestion du système**->**Authentification distante**->**Options** se compose des champs suivants :

Champs du menu Options globales RADIUS

Champ	Description
Authentification pour connexion PPP	Par défaut l'ordre d'authentification des connexions entrantes avec prise en compte de RADIUS est le suivant : d'abord CLID, puis PPP puis PPP avec RADIUS. Options : • *Inband* : Seules les requêtes Inband-RADIUS (PAP, CHAP, MS-CHAP V1 & V2) (c'est-à-dire requêtes PPP sans identification de numéro d'appel) sont envoyées au serveur RADIUS défini sous **Adresse IP du serveur**. • *Outband (CLID)* : Seules les requêtes Outband-RADIUS (c'est-à-dire requêtes d'identification des numéros d'appel) sont envoyées au serveur RADIUS (CLID = Calling Line Identification). Par défaut, l'option *Inband* est activée.

2.7 Accès à la configuration

Vous pouvez configurer les profils utilisateur dans le menu **Accès à la configuration**.

Pour cela, créez les profils d'accès et les utilisateurs, puis affectez l'utilisateur à au moins

un profil. Le profil d'accès donne accès à la partie de l'interface graphique dont l'utilisateur a besoin pour remplir ses tâches. Les parties non nécessaires sont bloquées.

2.7.1 Profils d'accès

Le menu **Gestion du système**->**Accès à la configuration**->**Profils d'accès** affiche une liste de tous les profils d'accès configurés. Le symbole vous permet de supprimer des entrées.

Pour **hybird 120** plusieurs profils sont déjà configurés par défaut. Vous pouvez les modifier à l'aide du symbole et restaurer les valeurs par défaut à l'aide du .

2.7.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Cliquez sur le bouton **Nouveau** pour créer d'autres profils d'accès.

Pour créer un profil d'accès, vous pouvez utiliser toutes les entrées qui se trouvent dans la barre de navigation du GUI et **Enregistrer la configuration** et **Basculer vers le navigateur SNMP**. Vous pouvez créer au plus 29 profils d'accès.

Le menu **Gestion du système**->**Accès à la configuration**->**Profils d'accès**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une désignation claire pour le profil d'accès.
Classe numéro	Le système attribue automatiquement au profil d'accès un numéro séquentiel. Celui-ci ne peut pas être modifié.

Champs du menu Touches

Champ	Description
Enregistrer la configuration	Si vous activez le bouton **Enregistrer la configuration**, l'utilisateur peut enregistrer les configurations. **Note** Attention, les mots de passe dans le fichier enregistré sont lisibles en clair.

Champ	Description
	Activez ou désactivez l'option **Enregistrer la configuration**. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Basculer vers le navigateur SNMP	Si vous activez le bouton **Basculer vers le navigateur SNMP**, l'utilisateur peut basculer dans la vue du navigateur SNMP, accéder aux paramètres et modifier tous ceux qui sont affichés. **Attention** Attention, l'autorisation pour **Basculer vers le navigateur SNMP** signifie que l'utilisateur peut accéder à la MIB complète, car il n'est pas possible de créer un profil d'accès individuel dans cette vue. L'autorisation pour **Enregistrer la configuration** lui permet d'enregistrer la MIB modifiée. L'autorisation pour **Basculer vers le navigateur SNMP** permet de lever à nouveau les limitations GUI configurées au niveau de la MIB. Activez ou désactivez l'option **Basculer vers le navigateur SNMP**. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Champs du menu Entrées de navigation

Champ	Description
Menus	Vous voyez tous les menus de la barre de navigation du GUI. Les menus qui contiennent au moins un sous-menu sont identifiés par ou . Le symbole identifie les pages. Lorsque vous créez un nouveau profil d'accès, aucun élément n'est encore affecté, c'est-à-dire que tous les menus, sous-menus et pages disponibles sont identifiés par le symbole . Chaque élément de la barre de navigation peut prendre trois

Champ	Description
	valeurs. Cliquez sur la ligne voulue sur le symbole pour afficher ces trois valeurs. Valeurs possibles : • *Refuser* : Le menu et tous ses sous-menus sont bloqués. • *Autoriser* : Le menu est débloqué. Les sous-menus doivent être débloqués séparément le cas échéant. • *Autoriser tout* : Le menu et tous ses sous-menus sont débloqués. Vous pouvez choisir dans la ligne *Autoriser* ou *Autoriser tout* pour affecter des éléments au profil d'accès en cours. Les éléments qui sont affectés au profil d'accès en cours sont identifiés par le symbole . identifie un menu bloqué dont au moins un des sous-menus est débloqué.

2.7.2 Utilisateur

Le menu **Gestion du système**->**Accès à la configuration**->**Utilisateur** affiche une liste de tous les utilisateurs configurés. Le symbole vous permet de supprimer des entrées.

Cliquez sur le bouton pour afficher les détails de l'utilisateur configuré. Vous voyez quels sont les champs et les menus qui lui sont attribués.

Le symbole signifie que **Lecture seule** est autorisé. Si une ligne est identifiée par le symbole , les informations sont accessibles en lecture et en écriture. Le symbole identifie les entrées bloquées.

2.7.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour saisir d'autres utilisateurs.

Le menu **Gestion du système**->**Accès à la configuration**->**Utilisateur**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Utilisateur	Saisissez une désignation claire pour l'utilisateur.
Mot de passe	Saisissez un mot de passe pour l'utilisateur.
L'utilisateur doit changer le mot de passe	L'option **L'utilisateur doit changer le mot de passe** permet à l'administrateur de définir si l'utilisateur doit fournir un mot de passe lors de la première connexion. Pour cela, l'option **Enregistrer la configuration** du menu **Profils d'accès** doit être active. Si cette option est inactive, un avertissement est affiché. Activez ou désactivez l'option **L'utilisateur doit changer le mot de passe**. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Niveau d'accès	Avec **Ajouter**, vous attribuez au moins un profil d'accès à l'utilisateur. En choisissant **Lecture seule**, l'utilisateur peut consulter les paramètres du profil d'accès, mais pas les modifier. La sélection **Lecture seule** est possible seulement si l'option**Basculer vers le navigateur SNMP** du menu **Profils d'accès** n'est pas active. Si l'option **Basculer vers le navigateur SNMP** est active, un avertissement est affiché, car l'utilisateur peut basculer dans la vue du navigateur SNMP, accéder aux paramètres et les modifier. L'option **Lecture seule** n'est pas disponible dans la vue du navigateur SNMP. Si l'utilisateur se voit attribuer des profils d'accès qui se chevauchent, l'option Lecture et écriture a une priorité supérieure à **Lecture seule**. Les boutons ne peuvent pas prendre la valeur **Lecture seule**.

2.8 Certificats

Un cryptosystème asymétrique sert à crypter les données qui sont transportées dans un réseau, à créer ou à vérifier des signatures numériques et à authentifier des utilisateurs. Le cryptage et le décryptage des données utilise une paire de clés, composée d'une clé publique et d'une clé privée.

Pour le cryptage, l'expéditeur a besoin de la clé publique du destinataire. Le destinataire décrypter les données avec sa clé privée. Pour être sur que la clé publique est légitime et

non piratée, un justificatif est requis, à savoir, un certificat numérique.

Un certificat numérique confirme entre autre l'authenticité et le propriétaire de la clé publique. On peut le comparer à un passeport officiel, qui confirme que le détenteur montre certaines caractéristiques, comme son sexe et son âge et que la signature est authentique. Compte tenu que les certificats ne sont pas délivrés par une seule autorité, comme le service des passeports, mais par différents organismes et avec une qualité différente, la notion de crédibilité de l'organe émetteur est centrale. La qualité d'un certificat est définie par ex. par la loi allemande sur la signature ou la directive européenne correspondante.

Les organismes de certification qui délivrent des certificats qualifiés sont organisés hiérarchiquement, l'agence fédérale des réseaux étant l'instance supérieure de certification. La structure et le contenu d'un certificat sont prédéfinis en fonction de la norme utilisée. X.509 est la norme la plus importante et la plus répandue pour les certificats numériques. Les certificats qualifiés sont personnels et particulièrement fiables.

Les certificats numériques sont partie prenante de l'infrastructure Public Key (PKI). On désigna par PKI un système qui peut délivrer, distribuer et vérifier des certificats numériques.

Les certificats sont délivrés pour une période donnée, généralement un an, c'est-à-dire que leur durée de validité et limitée.

Votre appareil est équipé pour utiliser des certificats pour les liaisons VPN et les liaisons vocales de type Voice over IP.

2.8.1 Liste de certificat

Le menu **Gestion du système**->**Certificats**->**Liste de certificat** affiche une liste de tous les certificats existants.

2.8.1.1 Editer

Cliquez sur le symbole pour consulter le contenu de l'objet sélectionné (clé, certificat ou requête).

Les certificats et les clés ne sont pas modifiables en soi, mais certains attributs externes peuvent être modifiés en fonction du type d'entrée sélectionnée.

Le menu **Gestion du système**->**Certificats**->**Liste de certificat**-> se compose des champs suivants :

Champs du menu Editer les paramètres

Champ	Description
Description	Affiche le nom du certificat, de la clé ou de la requête.
Le certificat est un certificat CA	Identifiez le certificat comme venant d'un organisme de certification (CA) fiable. Les certificats qui appartiennent à ce CA sont acceptés lors de l'authentification. Sélectionnez *Vrai* pour activer la fonction. La fonction est désactivée par défaut.
Vérification à partir d'une liste de blocage des certificats (CRL)	Uniquement pour **Le certificat est un certificat CA** = *Vrai* Définissez ici dans quelle mesure les listes de blocage (CRL) doivent être incluses dans la validation des certificats émis par leurs propriétaires. Réglages possibles : • *Désactivé*: Pas de vérification des CRL. • *Toujours*: les CRL sont vérifiées de manière approfondie. • *Uniquement s'il existe un point de répartition des listes de blocage de certificat* (valeur par défaut) : Il n'y a vérification que si le certificat contient une entrée CRL-Distribution-Point. Ceci peut être vérifié dans le contenu du certificat sous « Afficher les détails ». • *Utiliser les paramètres du certificat de niveau supérieur* : Les paramètres du certificat de niveau supérieur sont utilisés le cas échéant. Sinon, la procédure est la même que pour « Uniquement s'il existe un point de répartition des listes de blocage de certificat ».
Forcer la fiabilité du certificat	Définissez que ce certificat doit être accepté comme certificat de l'utilisateur sans autre vérification lors de l'authentification. Sélectionnez *Vrai* pour activer la fonction. La fonction est désactivée par défaut.

Attention

Il est fondamental pour la sécurité d'un VPN que l'intégrité de tous les certificats marqués manuellement comme fiables (certificats des organes de certification et certificats de l'utilisateur) soit effectivement garantie. Les « Fingerprints » (empreintes digitales) affichés peuvent être utilisés pour vérifier cette intégrité : Comparez les valeurs affichées avec les Fingerprints que l'émetteur du certificat (p.ex. sur Internet) a fourni. Il suffit pour cela de vérifier une des deux valeurs.

2.8.1.2 Demande de certificat

Certificats Registration-Authority dans SCEP

En cas d'utilisation de SCEP (Simple Certificate Enrollment Protocol), votre appareil prend en charge également des certificats Registration-Authority distincts.

Les certificats Registration-Authority sont utilisés par certains organismes de certification (Certificate Authorities ou CA) pour traiter certaines tâches (signature et cryptage) pendant la communication SCEP avec des clés distinctes et déléguer la procédure le cas échéant à des organismes d'enregistrement (Registration Authorities)séparés.

En cas de téléchargement automatique d'un certificat, c'est-à-dire quand **Certificat CA** = *-- Téléchargement --* est sélectionné, tous les certificats requis pour la procédure sont chargés automatiquement.

Si tous les certificats requis sont déjà dans le système, ils peuvent aussi être sélectionnés manuellement.

Sélectionnez le bouton **Demande de certificat** pour demander ou pour importer d'autres certificats.

Le menu **Gestion du système**->**Certificats**->**Liste de certificat**->**Demande de certificat** se compose des champs suivants :

Champs du menu Demande de certificat

Champ	Description
Description de la demande de certificat	Saisissez une désignation claire pour le certificat.
Mode	Indiquez comment vous voulez demander le certificat. Sont disponibles :

Champ	Description
	• *Manuel* (valeur par défaut) : Votre appareil crée pour la clé un fichier PKCS#10 qui est chargé directement dans le navigateur ou copié dans le menu via le champ **Afficher les détails**. Ce fichier doit être remis au CA et le certificat reçu est importé manuellement sur l'appareil. • *SCEP* : La clé est demandée à un CA au moyen du Simple Certificate Enrollment Protocol.
Générer une clé privée	Uniquement pour **Mode** = *Manuel* Sélectionnez un algorithme pour la création de la clé. Sont disponibles les valeurs *RSA* (par défaut) et *DSA*. Sélectionnez de plus la longueur de la clé à créer. Valeurs possibles : *512*, *768*, *1024*, *1536*, *2048*, *4096*. Attention, une clé de 512 bits est considérée comme non sure, alors qu'une clé de 4 096 bits est non seulement longue à créer, mais aussi occupe pendant le traitement IPSec une bonne partie des ressources. Une valeur de 768 ou plus est cependant recommandée, la valeur par défaut est 1 024 bits.
URL SCEP	Uniquement pour **Mode** = *SCEP* Saisissez l'URL du serveur SCEP, p. ex. http://scep.beispiel.com:8080/scep/scep.dll Les données correspondantes vous sont transmises par votre administrateur CA.
Certificat CA	Uniquement pour **Mode** = *SCEP* Sélectionnez le certificat CA. • *-- Téléchargement --* : Saisissez le nom du certificat CA dans le champ **Nom CA** de l'organisme de certification (CA) à qui vous demandez votre certificat, p. ex. *cawindows*. Les données correspondantes vous sont transmises par votre administrateur CA. S'il n'existe pas de certificat CA, l'appareil télécharge d'abord le certificat CA de l'organisme CA. Il poursuit avec

Champ	Description
	l'enregistrement s'il ne manque pas de paramètres essentiels. Dans ce cas, il revient dans le menu **Générer une demande de certificat**. Si le certificat CA ne contient pas de poste de répartition CRL (Certificate Revocation List, CRL) et s'il n'y a pas de serveur de certificat configuré sur l'appareil, ce CA ne vérifie pas la validité de ce certificat. • <Nom d'un certificat existant> : Si tous les certificats requis sont déjà dans le système, ils peuvent être sélectionnés manuellement.
Certificat de signature RA	Uniquement pour **Mode** = *SCEP* Uniquement pour **Certificat CA** non = *-- Téléchargement --* Sélectionnez un certificat pour la signature de la communication SCEP. La valeur par défaut est *-- Utiliser le certificat CA --*, c'est-à-dire que le certificat CA est utilisé.
Certificat d'encryptage RA	Uniquement pour **Mode** = *SCEP* Uniquement si **Certificat de signature RA** non = *-- Utiliser le certificat CA --* Si vous utilisez un certificat propre pour la signature de la communication avec le RA, vous pouvez ici sélectionner un autre cryptage de la communication. La valeur par défaut est *-- Utiliser le certificat de signature RA --*, c'est-à-dire qu'on utilise le même certificat CA que pour la signature.
Mot de passe	Uniquement pour **Mode** = *SCEP* Afin d'obtenir des certificats pour votre clé, vous pouvez avoir besoin d'un mot de passe délivré par l'organisme de certification. Saisissez ici le mot de passe qui vous a été octroyé par votre organisme de certification.

Champs du menu Nom de l'objet

Champ	Description
Personnalisé	Indiquez si les composants de nom du sujet doivent être saisis séparément en fonction des prescriptions du CA ou s'il faut saisir un nom de sujet spécial. Si *Activé* est sélectionné, il est possible de saisir dans **Résumé** un nom de sujet avec attributs qui n'est pas proposé dans la liste. Exemple : « CN=VPNServer, DC=mydomain, DC=com, c=DE ». Si ce champ n'est pas marqué, saisissez les composants de nom dans **Nom général**, **E-mail**, **Unité organisationnelle**, **Organisation**, **Lieu**, **Etat/Province** et **Pays**. La fonction est désactivée par défaut.
Résumé	Uniquement pour **Personnalisé** = activé. Saisissez un nom de sujet avec attributs qui n'est pas proposé dans la liste. Exemple : « CN=VPNServer, DC=mydomain, DC=com, c=DE ».
Nom général	Uniquement pour **Personnalisé** = désactivé. Saisissez le nom fourni par le CA.
E-mail	Uniquement pour **Personnalisé** = désactivé. Saisissez l'adresse mail fournie par le CA.
Unité organisationnelle	Uniquement pour **Personnalisé** = désactivé. Saisissez l'unité organisationnelle fournie par le CA.
Organisation	Uniquement pour **Personnalisé** = désactivé. Saisissez l'organisation fournie par le CA.
Lieu	Uniquement pour **Personnalisé** = désactivé. Saisissez le lieu fourni par le CA.
Etat/Province	Uniquement pour **Personnalisé** = désactivé.

Champ	Description
	Saisissez l'état/la région fourni par le CA.
Pays	Uniquement pour **Personnalisé** = désactivé. Saisissez le pays fourni par le CA.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Noms alternatifs sujet

Champ	Description
#1, **#2**, **#3**	Définissez pour chaque entrée le type du nom de saisissez les noms de sujet supplémentaire. Valeurs possibles : • *aucun* (valeur par défaut) : Aucun nom supplémentaire n'est saisi. • *IP* : Une adresse IP est saisie. • *DNS* : Un nom DNS est saisi. • *E-mail* : Une adresse mail est saisie. • *URI* : Un Uniform Resource Identifier est saisi. • *DN* : Un Distinguished Name (DN) est saisi. • *RID* : Un Registered Identity (RID) est saisi.

Champ du menu Options

Champ	Description
Mode enregistrement automatique	Indiquez si votre appareil enregistre automatiquement en interne les différentes étapes du processus d'enregistrement. Ceci est utile lorsque l'enregistrement ne peut pas être terminé tout de suite. Si l'état n'a pas été enregistré, l'enregistrement incomplet ne peut pas être terminé. Dès que l'enregistrement est terminé et que le certificat a été téléchargé depuis le serveur CA, il est automatiquement enregistré dans la configuration de votre appareil. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

2.8.1.3 Importer

Sélectionnez le bouton **Importer** pour importer un certificat.

Le menu **Gestion du système**->**Certificats**->**Liste de certificat**->**Importer** se compose des champs suivants :

Champs du menu Importer

Champ	Description
Nom de fichier externe	Saisissez le chemin d'accès et le nom de fichier du certificat qui doit être importé ou sélectionnez le fichier avec **Rechercher...** via le navigateur du fichier.
Description de certificat locale	Saisissez une désignation claire pour le certificat.
Encodage du fichier	Choisissez le type de codage, de sorte que l'appareil puisse décoder le certificat. Valeurs possibles : • *Auto* (valeur par défaut) : Permet d'activer la détection automatique de codage. En cas d'échec du téléchargement du certificat en mode automatique, essayez un codage spécifique. • *Base64* • *Binaire*
Mot de passe	Afin d'obtenir des certificats pour votre clé, vous pouvez avoir besoin d'un mot de passe. Saisissez le mot de passe.

2.8.2 CRL

Le menu **Gestion du système**->**Certificats**->**CRL** affiche une liste de tous les CRL (Certificate Revocation List).

Si une clé ne peut plus être utilisée, p. ex. parce qu'elle a été dévoyée ou perdue, ce certificat est déclaré invalide. L'organisme de certification annule le certificat, il publie les listes de certificats bloqués, les CRL. Les utilisateurs des certificats doivent toujours contrôler ces listes pour vérifier le certificat utilisé. Cette procédure de vérification peut être auto-

matisée via un navigateur.

Le Simple Certificate Enrollment Protocol (SCEP) prend en charge la publication et la révocation des certificats dans les réseaux.

2.8.2.1 Importer

Sélectionnez le bouton **Importer** pour importer des CRL.

Le menu **Gestion du système**->**Certificats**->**CRL**->**Importer** se compose des champs suivants :

Champs du menu Importation CRL

Champ	Description
Nom de fichier externe	Saisissez le chemin d'accès et le nom de fichier du CRL qui doit être importé ou sélectionnez le fichier avec **Rechercher...** via le navigateur du fichier.
Description de certificat locale	Saisissez une désignation claire pour les CRL.
Encodage du fichier	Choisissez le type de codage, de sorte que l'appareil puisse décoder les CRL. Valeurs possibles : • *Auto* (valeur par défaut) : Permet d'activer la détection automatique de codage. En cas d'échec du téléchargement des CRL en mode automatique, essayez un codage spécifique. • *Base64* • *Binaire*
Mot de passe	Saisissez le mot de passe à importer.

2.8.3 Serveur de certificat

Le menu **Gestion du système**->**Certificats**->**Serveur de certificat** affiche une liste de tous les serveurs de certificats.

Un organisme de certification (fournisseur de service de certification, Certificate Authority, CA) fournit vos certificats aux clients qui le demandent, via un serveur de certification. Le serveur de certificats publie également les clés privées et fournit les listes de blocage des

certificats (CRL) qui sont interrogées pour la vérification des certificats soit par LDAP ou par HTTP.

2.8.3.1 Nouveau

Sélectionnez le bouton **Nouveau** pour créer un serveur de certificats.

Le menu **Gestion du système**->**Certificats**->**Serveur de certificat**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une désignation claire pour le serveur de certificats.
Chemin d'accès URL LDAP	Saisissez l'URL LDAP ou HTTP du serveur.

Chapitre 3 Interfaces physiques

3.1 Ports Ethernet

Une interface Ethernet est une interface physique pour la connexion au réseau local ou à des réseaux externes.

A la livraison, les ports Ethernet **ETH1** à **ETH4** sont affectés à une seule interface Ethernet logique. L'interface Ethernet logique *en1-0* est affectée et préconfigurée avec l'**Adresse IP** *192.168.0.250* et le **Masque réseau** *255.255.255.0*.

Le port **ETH5** est affecté à l'interface Ethernet *en1-4* et n'est pas préconfiguré.

Note

Pour assurer l'accessibilité de votre système, vous devez veiller lors de la distribution des ports à ce que l'interface Ethernet *en1-0* avec l'adresse IP et le masque de réseau préconfigurés soit affectée à un port accessible par Ethernet. Le cas échéant, réalisez la configuration par connexion sérielle via l'interface **Serial 1**.

ETH1 - ETH4

Les interfaces peuvent être utilisées individuellement. Elles sont séparées logiquement en affectant à chaque port à l'aide du menu **Configuration du port** dans le champ **Sélection de l'interface Ethernet** l'interface Ethernet logique souhaitée. Pour chaque interface Ethernet affectée, le menu **LAN**->**Configuration IP** affiche une nouvelle interface dans la liste et permet une configuration entièrement individuelle de l'interface.

ETH5

Par défaut, l'interface Ethernet logique *en1-4* est affectée au port **ETH5**. Les options de configuration sont identiques à celles des ports **ETH1** - **ETH4**.

VLAN pour interfaces de routage

Configurez les VLAN par ex. pour séparer des segments de réseau individuels (par ex. plusieurs services d'une entreprise) ou pour procéder à la réservation de bande passante pour certains VLAN lors de l'utilisation de Managed Switches avec fonction QoS.

3.1.1 Configuration du port

Séparation des ports

Votre appareil vous permet d'exploiter les ports de switch en tant qu'interfaces et de les séparer logiquement, pour les configurer en tant qu'interfaces Ethernet individuelles.

Lors de la configuration, vous devez tenir compte des points suivants : La répartition des ports de switch sur plusieurs interfaces Ethernet ne sépare celles-ci que sur le plan logique. La largeur de bande passante totale disponible de max. 1 000 Mbits/s FullDuplex pour toutes les interfaces générées ne change pas. Si vous séparez donc tous les ports de switch, chacune des interfaces générées ne dispose que d'une partie de la bande passante intégrale. Si vous regroupez plusieurs ports de switch en une interface, les ports bénéficient ensemble de la largeur passante complète de max. 1 000 Mbits/s Full Duplex.

Le menu **Interfaces physiques**->**Ports Ethernet**->**Configuration du port** se compose des champs suivants :

Champs du menu Configuration Switch

Champ	Description
Port Switch	Affiche le port de switch respectif. La numérotation correspond à la numérotation des ports Ethernet au dos de l'appareil.
Sélection de l'interface Ethernet	Affectez au port de switch respectif une interface Ethernet logique. Cinq interfaces sont disponibles au choix, de *en1-0* à *en1-2*. Dans la configuration de base, le port de switch **1**-**4** est affecté à l'interface *en1-0*.
Vitesse configurée/ Mode configuré	Sélectionnez le mode dans lequel l'interface doit être exploitée. Valeurs possibles : • *Négociation entièrement automatique* (valeur par défaut) • *Auto 1000 Mbits/s only* • *Auto 100 Mbits/s only* • *Auto 10 Mbits/s only* • *Auto 100 Mbits/s / Full Duplex* • *Auto 100 Mbits/s / Half Duplex*

Champ	Description
	• *Auto 10 Mbits/s / Full Duplex* • *Auto 10 Mbits/s / Half Duplex* • *Fixe 1000 Mbits/s / Full Duplex* • *Fixe 100 Mbits/s / Full Duplex* • *Fixe 100 Mbits/s / Half Duplex* • *Fixe 10 Mbits/s / Full Duplex* • *Fixe 10 Mbits/s / Half Duplex* • *aucun* : L'interface est créée, mais reste inactive.
Vitesse actuelle/Mode actuel	Affiche le mode réel et la vitesse réelle de l'interface. Valeurs possibles : • *1000 Mbits/s / Full Duplex* • *100 Mbits/s / Full Duplex* • *100 Mbits/s / Half Duplex* • *10 Mbits/s / Full Duplex* • *10 Mbits/s / Half Duplex* • *Inactif*
Contrôle de flux	Choisissez si un contrôle de flux doit être réalisé pour l'interface correspondante. Valeurs possibles : • *Désactivé* (valeur par défaut) : Aucun contrôle de flux n'est effectué. • *Activé* : Un contrôle de flux est effectué. • *Auto* : Un contrôle de flux automatique est effectué.

3.2 Ports RNIS

Les connecteurs RNIS du système peuvent être configurés aux choix comme connecteurs RNIS internes ou externes. Les connecteurs RNIS externes servent à la connexion au réseau RNIS du fournisseur de réseau. Les connexions RNIS internes sont prévues pour la connexion de différents terminaux RNIS (téléphones systèmes, téléphones RNIS, etc).

3.2.1 RNIS externe

Le menu **Interfaces physiques**->**Ports RNIS**->**RNIS externe** vous permet de configurer les connexions RNIS externes de votre système.

Le type de connexion d'une connexion RNIS externe est réglable en connexion multipostes (P-MP) ou connexion d'installation (P-P).

Lors du raccordement à plusieurs connexions RNIS, les variantes suivantes sont possibles :

- Toutes les connexions RNIS externes sont des connexions multipostes (P-MP).
- Toutes les connexions RNIS externes sont des connexions d'installation (P-P).
- Les connexions RNIS externes sont des connexions multipostes (P-MP) et des connexions d'installation (P-P).

3.2.1.1 Editer avec

Sélectionnez le bouton pour traiter une entrée.

Le menu **Interfaces physiques**->**Ports RNIS**->**RNIS externe**-> se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description personnalisée de l'interface RNIS. La valeur par défaut est *RNIS externe*.
Nom	Permet d'afficher la désignation de l'interface RNIS. Valeurs possibles : • *S/U* : 4 fils (S) • */*: permet d'afficher le port sur le module auquel l'interface RNIS est raccordée. Exemple : *S/U 1* = l'interface se trouve sur le port 1 et est utilisée comme connexion S.
Type de connexion	Choisissez si l'interface RNIS doit être exploitée en tant que connexion multipostes ou connexion d'installation.

Champ	Description
	Valeurs possibles : • *Connexion de l'installation* (valeur par défaut) • *Connexion multi-appareils*

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Maintenir le niveau 2 actif en permanence	Cette fonction (appelée aussi surveillance continue) surveille en continu l'opérationnalité et la qualité de transmission d'une connexion RNIS externe. A cet effet, le système est continuellement en contact avec le central de votre fournisseur de réseau. Si le niveau RNIS 2 n'est pas maintenu en activité continue par le central, le système peut initier la constitution répétée du niveau 2. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Couche 1 synchronisation permanente	Lors de la connexion d'un appareil externe (par ex. une passerelle GSM) au connecteur d'installation externe du système, le cycle de l'appareil externe peut provoquer des dysfonctionnements de la synchronisation du cycle de l'installation. Nous vous recommandons de ne désactiver la synchronisation du niveau 1 que dans le cas d'un tel dysfonctionnement. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

3.2.2 RNIS interne

Le menu **Interfaces physiques**->**Ports RNIS**->**RNIS interne** vous permet de configurer les interfaces RNIS internes de votre système.

Les connexions RNIS internes sont toujours des connexions multipostes.

Lors de la connexion de terminaux à une connexion RNIS interne, il convient de ne pas oublier que certains terminaux RNIS proposés dans le commerce ne sont pas en mesure d'exécuter à l'aide de leurs touches les fonctions mises à disposition par votre système.

Le menu **Interfaces physiques**->**Ports RNIS**->**RNIS interne** se compose des champs suivants :

Champs du menu RNIS interne

Champ	Description
Nom	Permet d'afficher la désignation de l'interface RNIS. Valeurs possibles : • *S/U* : 4 fils (S) • */*: permet d'afficher le port sur le module auquel l'interface RNIS est raccordée. Exemple : *S/U 2* = l'interface se trouve sur le port 2 et est utilisée comme connexion S.
Fonction	Affiche la fonction de l'interface RNIS. Valeurs possibles : • *Upn*: Interface pour terminaux CAPI. • *Upn*: Interface pour terminaux UPN. • *S0*: Interface pour connecteur RNIS-S0.
MSN par défaut	Affiche si une MSN standard a été affecté à un bus S0 interne. Une MSN standard permet d'accéder à des terminaux S0 non configurés. Comme MSN standard, vous pouvez utiliser des numéros d'appels internes qui sont configurés dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur** et affectés à un terminal dans le menu **Appareil terminal**.
État	Permet d'afficher l'état de l'interface.

3.2.2.1 Editer

Sélectionnez le bouton pour traiter une entrée.

Le menu **Interfaces physiques**->**Ports RNIS**->**RNIS interne**-> se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
MSN par défaut	Sélectionnez le numéro d'appel souhaité. Vous pouvez choisir parmi les numéros d'appel que vous avez configurées dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Numéros d'appel**. Valeurs possibles : • *Non configuré* • *<Numéro d'appel>*

3.3 Ports analogiques

3.3.1 Analogue externe (FXO)

Le menu **Analogue externe (FXO)** affiche toutes les connexions externes analogiques disponibles de votre système.

Le menu **Interfaces physiques**->**Ports analogiques**->**Analogue externe (FXO)** se compose des champs suivants :

Valeurs de la liste Analogue externe (FXO)

Champ	Description
Nom	Permet d'afficher la désignation de l'interface analogique. Valeurs possibles : • *FXO*: Désignation de la connexion analogique.
Description	Permet d'afficher la description personnalisée de l'interface analogique.
Méthode de numérotation	Permet d'afficher la procédure de sélection utilisée. Valeurs possibles : • *Signalisation multifréquence (DTMF)* (valeur par défaut) • *Impulsions de numérotation (IWV)*

Champ	Description
État	Permet d'afficher l'état de l'interface.
Action	Le statut de l'interface est modifié en actionnant le bouton ou le bouton dans la colonne **Action**.

3.3.1.1 Editer

Sélectionnez le bouton pour traiter une entrée.

Le menu **Interfaces physiques**->**Ports analogiques**->**Analogue externe (FXO)**-> se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description personnalisée de l'interface analogique.
Nom	Permet d'afficher la désignation de l'interface analogique. Valeurs possibles : • *FXO*: Désignation de la connexion analogique.
Méthode de numérotation	Indiquez quelle procédure de sélection doit être utilisée. Valeurs possibles : • *Signalisation multifréquence (DTMF)* (valeur par défaut) • *Impulsions de numérotation (IWV)*
CLIP	Choisissez si la caractéristique de performances CLIP doit être utilisée, c'est-à-dire si le numéro d'appel de l'appelant doit s'afficher sur le poste de l'appelé. Valeurs possibles : • *Arrêt* (valeur par défaut) : Le numéro d'appel de l'appelant ne s'affiche pas sur le poste de l'appelé. • *FM*: Les données sont envoyées en tant que DTMF.

Champ	Description
Recevoir les informations sur les coûts	Choisissez si votre appareil doit recevoir des données de coûts depuis le réseau. Vous pouvez déterminer si l'impulsion de taxation doit s'élever à 12 ou à 16 kHz. Valeurs possibles : • *Désactivé* (valeur par défaut) : Les données de coûts ne sont pas reçues. • *12 kHz* • *16 kHz*

Champs du menu Paramètres étendus

Champ	Description
Détection de la sonnerie occupé	Indiquez si **Détection de la sonnerie occupé** doit être utilisé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Détection de la sonnerie de numérotation	Indiquez si **Détection de la sonnerie de numérotation** doit être utilisé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut. Si la **Détection de la sonnerie de numérotation** est active et que la tonalité de numérotation externe est détectée, votre **hybird 120** lance immédiatement la numérotation.
Pause sonnerie de numérotation	Uniquement en cas de **Détection de la sonnerie de numérotation** désactivée. Saisissez la valeur souhaitée que le système doit attendre au maximum lors de la numérotation d'un numéro de téléphone jusqu'à ce qu'il lance la numérotation. La **Pause sonnerie de numérotation** peut être activée lorsque votre **hybird 120** ne détecte pas la tonalité de numérotation ou qu'aucune tonalité de numérotation n'est transmise. Vous devez déterminer vous-même la **Pause sonnerie de numérotation**.

Champ	Description
	Les valeurs possibles sont des valeurs entières entre *1* seconde et *5* secondes.
Temps de surveillance de fin de numérotation	Saisissez le temps que le système doit attendre après la sélection d'un chiffre avant de considérer le numéro de téléphone comme complet et d'établir la connexion. La valeur par défaut est *5* secondes.

3.3.2 Analogue interne (FXS)

Le menu **Analogue interne (FXS)** affiche toutes les connexions internes analogiques disponibles de votre système.

Le menu **Interfaces physiques**->**Ports analogiques**->**Analogue interne (FXS)** se compose des champs suivants :

Valeurs de la liste Analogue interne (FXS)

Champ	Description
Nom	Permet d'afficher la désignation de l'interface analogique. Valeurs possibles : • *FXS*: Désignation de la connexion analogique.
Fonction	Permet d'afficher la fonction de l'interface analogique. Valeurs possibles : • *Téléphone* • *Adaptateur TFE* • *Appareil multifonctions/télécopieur* • *Modem* • *Répondeur* • *Téléphone d'urgence* La fonction du terminal analogique est configurée dans le menu **Appareil terminal**->**Autres téléphones**->**analogue**.
État	Permet d'afficher l'état de l'interface.

Chapitre 4 VoIP

Voice over IP (VoIP) utilise le protocole IP pour la transmission vocale et d'images.

A la grande différence de la téléphonie traditionnelle, les informations vocales ne sont pas transmises via une communication commutée sur un réseau téléphonique, mais bien réparties via le protocole IP en paquets de données atteignant leur destination de manière non définie sur un réseau. Cette technologie se sert ainsi de l'infrastructure d'un réseau existant pour permettre la transmission vocale et partage ce réseau avec d'autres services de communication.

4.1 Paramètres

Le menu **VoIP**->**Paramètres** permet de configurer vos connexions VoIP.

Vous avez la possibilité d'établir une communication téléphonique via Internet avec tous les téléphones connectés en interne. Le nombre de connexions dépend de différents paramètres :

- La disponibilité des canaux au sein du système.
- La bande passante de la connexion DSL disponible.
- Les fournisseurs SIP configurés et disponibles.
- Les licences de sortie SIP entrées.

4.1.1 Fournisseur SIP

Le menu **VoIP**->**Paramètres**->**Fournisseur SIP** permet de configurer les fournisseurs SIP de votre choix.

Appuyez sur le bouton ou dans la colonne **Action** pour modifier l'état du fournisseur SIP.

Après environ une minute, l'enregistrement est effectué auprès du fournisseur et le statut est automatiquement défini sur (actif).

4.1.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **VoIP**->**Paramètres**->**Fournisseur SIP**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Vous pouvez entrer une désignation pour le fournisseur SIP. Il est possible d'utiliser une suite de 20 caractères alphanumériques.
État du fournisseur	Indiquez si cette entrée de fournisseur VoIP doit être active (*active*, valeur par défaut) ou non (*inactive*).
Type de connexion	Sélectionnez le type de numéro d'appel VoIP à configurer. Valeurs possibles : • *Numéro d'appel unique* (valeur par défaut) : saisissez plusieurs numéros d'appel VoIP. • *Indicatif* : saisissez un numéro de base lié à un bloc de numéros d'appel.
ID d'authentification	Indiquez l'ID d'authentification de votre fournisseur. Il est possible d'utiliser une suite de 64 caractères alphanumériques.
Mot de passe	Vous pouvez attribuer un mot de passe à cet endroit. Il est possible d'utiliser une suite de 32 caractères alphanumériques.
Nom de l'utilisateur	Indiquez le nom d'utilisateur que vous a fait parvenir votre fournisseur VoIP. Il est possible d'utiliser une suite de 64 caractères alphanumériques.
Domaine	Saisissez un autre nom de domaine ou une autre adresse IP du serveur proxy SIP. En l'absence de saisie, l'entrée est utilisée dans le champ **Registrar**. Remarque : saisissez ensuite un seul nom ou une seule adresse IP explicitement prédéfini(e) par votre fournisseur.

Champs du menu Paramètres pour numéro d'appel sortant

Champ	Description
Numéro d'appel sortant	Sélectionnez la signalisation souhaitée pour les appels vers l'extérieur. Valeurs possibles : • *Standard* (valeur par défaut) • *Numéro d'appel global pour CLIP-No-Screening* • *Numéro d'appel personnel pour CLIP-No-Screening* • *DDI fixe vers externe* (Uniquement pour **Type de connexion** = *numérotation directe*)
Numéro d'appel global pour CLIP-No-Screening	Uniquement pour **Numéro d'appel sortant** *Numéro d'appel global pour CLIP-No-Screening* Indiquez le numéro d'appel devant être visible par les personnes appelées dans le cadre de communications vers l'extérieur. Ce numéro d'appel n'est pas vérifié.
Afficher le numéro d'appel de l'interlocuteur distant	Uniquement pour **Numéro d'appel sortant** = *Numéro d'appel global pour CLIP-No-Screening* et *Numéro d'appel personnel pour CLIP-No-Screening* Vous pouvez afficher le numéro d'appel d'un interlocuteur externe, dans la mesure où il est signalé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Afficher le numéro d'appel fixe pour les communications sortantes	Uniquement pour **Numéro d'appel sortant** = *DDI fixe vers externe* Indiquez le numéro d'appel devant être visible par les personnes appelées dans le cadre de communications vers l'extérieur.

Champs du menu Registrar

Champ	Description
Registrar	Indiquez le nom DNS ou l'adresse IP du serveur SIP. Il est

Champ	Description
	possible d'utiliser une suite de 26 caractères alphanumériques.
Port Registrar	Indiquez le numéro du port à utiliser pour la connexion au serveur. La valeur définie par défaut est *5060*. Il est possible d'utiliser une suite de 5 chiffres.
Protocole transparent	Sélectionnez le protocole transparent pour cette communication. Valeurs possibles : • *UDP* (valeur par défaut) • *TCP*

Champs du menu STUN

Champ	Description
Serveur STUN	Saisissez le nom ou l'adresse IP du serveur STUN. STUN = Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NAT) Un serveur STUN est nécessaire pour permettre aux appareils VoIP situés derrière un routeur NAT actif d'accéder à Internet. Dans ce cas, l'adresse IP publique actuelle de la connexion est déterminée et utilisée pour garantir un adressage précis de l'extérieur. Nombre maximum de caractères : 32.
Port serveur STUN	Saisissez le numéro du port à utiliser pour la connexion au serveur STUN. La valeur définie par défaut est *3478*. Il est possible d'utiliser une suite de 5 chiffres.

Champs du menu Horloge

Champ	Description
Horloge d'enregistrement	Saisissez ici le délai en secondes avant l'écoulement duquel le client SIP doit se réenregistrer afin que la connexion ne soit pas automatiquement interrompue. La valeur définie par défaut est *60*.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Proxy	Indiquez le nom DNS ou l'adresse IP du serveur SIP. Il est possible d'utiliser une suite de 26 caractères alphanumériques.
Port Proxy	Saisissez le numéro du port à utiliser pour la connexion au proxy. La valeur définie par défaut est *5060*. Il est possible d'utiliser une suite de 5 chiffres.
Protocole transparent	Sélectionnez le protocole transparent pour cette communication. Valeurs possibles : • *UDP* (valeur par défaut) • *TCP*

Champs du menu Autres paramètres

Champ	Description
From Domain	Saisissez le « From Domain » de votre fournisseur SIP. Celui-ci est utilisé comme information d'envoi dans l'en-tête SIP des paquets de données SIP, après le symbole @.
Nombre de communications simultanées admises	Sélectionnez le nombre maximal de communications qu'il doit être possible d'établir simultanément. Tenez également compte des paramètres de gestion de la bande passante. Valeurs possibles : • *Illimité* (valeur par défaut) : le nombre de conversations simultanées possibles est illimité. • *1* • *2* • *3* • *4* • *5* • *10*
Emplacement	Sélectionnez l'emplacement du serveur SIP. Le menu

Champ	Description
	Paramètres->**Emplacements** permet de définir les emplacements. Valeurs possibles : • *Tous les emplacements* (valeur par défaut) : le serveur n'est pas utilisé à un emplacement défini. • *<Nom de l'emplacement>*
Profils Codec	Sélectionnez le profil Codec pour ce serveur SIP. Le menu **VoIP**->**Paramètres**->**Profils Codec** permet de définir les profils Codec. Valeurs possibles : • *Système par défaut* (valeur par défaut) : le serveur fonctionne avec un profil Codec prédéfini dans le système. • *<Nom du profil Codec>*
Horloge de surveillance de fin de numérotation	Sélectionnez, en secondes, le délai (après la numérotation du dernier chiffre d'un numéro d'appel) après lequel le système commence la numérotation externe. La valeur par défaut est *5*.
Arrêt dans le système	Indiquez si une conversation téléphonique peut être mise en attente dans le système sans perdre la connexion (questions/défauts). Si cette fonction est désactivée, l'appel auprès du fournisseur SIP est mis en attente, à condition que ce fournisseur prenne en charge cette fonctionnalité. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Transfert des appels externe (SIP 302)	Indiquez si un appel est transféré vers l'extérieur auprès du fournisseur SIP. L'appel est transféré à l'aide du code d'état SIP 302. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Créer un numéro d'appel international	Si vous avez activé cette fonction et entré sous **Paramètres globaux** le **Réglage du pays** (*49* pour l'Allemagne), la suite de chiffres 0049 est générée automatiquement devant un numéro d'appel composé avec préfixe.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Créer un numéro d'appel national	Si vous avez activé cette fonction et saisi sous **Paramètres globaux** le **Préfixe national/Indicatif réseau local** (*40* pour Hambourg, p. ex.) le préfixe 040 est automatiquement généré devant le numéro d'appel composé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Désactiver la désactivation du numéro	Si vous activez cette fonction, le numéro d'appel est toujours envoyé, que vous ayez activé la fonction **Masquer le numéro d'appel A (CLIR)** auprès d'un abonné ou non. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Champs d'en-tête SIP pour le nom d'utilisateur	Sélectionnez la position du nom de l'utilisateur (ID utilisateur) dans l'en-tête SIP pour les appels sortants. Valeurs possibles : • *P-Preferred* : l'en-tête SIP est élargi par le champ « p-preferred-identity » pour y insérer le **Nom de l'utilisateur**. • *P-Asserted* : l'en-tête SIP est élargi par le champ « p-asserted-identity » pour y insérer le **Nom de l'utilisateur**. • *Aucun* : le **Nom de l'utilisateur** n'est pas inséré.
Champs d'en-tête SIP pour adresse d'appel	Sélectionnez la position de l'ID de l'expéditeur (p. ex. numéro d'appel) dans l'en-tête SIP pour les appels sortants. (Le numéro d'appel est automatiquement défini à partir de l'en-tête SIP pour les appels entrants.) Valeurs possibles : • *Affichage*: l'ID de l'expéditeur est inséré dans l'en-tête SIP du champ « Display ». • *Nom de l'utilisateur* : l'ID de l'expéditeur est inséré

Champ	Description
	dans l'en-tête SIP du champ « User ». • *P-Preferred* : l'en-tête SIP est élargi par le champ « p-preferred-identity » pour y insérer l'ID de l'expéditeur. • *P-Asserted* : l'en-tête SIP est élargi par le champ « p-asserted-identity » pour y insérer l'ID de l'expéditeur.
Remplacer le préfixe international par "+"	Indiquez si le préfixe (p. ex. 00) doit être remplacé par « + » dans le cas de numéros d'appel internationaux. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Autoriser la connexion d'un proxy	Indiquez si un autre système de télécommunications peut être enregistré sur votre système. Plusieurs systèmes de télécommunications peuvent ainsi être couplés. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Supprimer les liaisons SIP après le redémarrage	Si, p. ex., une réinitialisation du système ou une coupure de courant se produit après l'enregistrement d'un fournisseur, il se peut qu'il ne soit plus possible d'effectuer un nouvel enregistrement en fonction du fournisseur. L'activation de cette fonctionnalité permet d'effectuer un nouvel enregistrement après un redémarrage. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Appareil en amont avec NAT	L'activation de cette fonction vous permet d'utiliser un appareil en amont avec NAT tout en ayant la possibilité de téléphoner avec VoIP. Sans cette fonction, vous ne pouvez recevoir aucun appel via VoIP lors de l'utilisation d'un appareil en amont avec NAT. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Prise en charge Early-Media	Indiquez si vous souhaitez autoriser l'échange de données audio ou vocales avant qu'un destinataire ne réponde à un appel.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Fournisseur sans enregistrement	Indiquez s'il est nécessaire ou non de procéder à l'enregistrement et à l'authentification auprès d'un fournisseur. Dans ce cas, les données pertinentes sont envoyées à une adresse IP qui est déjà connue des partenaires de connexion. Microsoft Exchange SIP illustre cette procédure. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Si la fonction est désactivée, une authentification a lieu par défaut. Dans ce cas, chaque client SIP (utilisateur) signale sa position actuelle à un serveur Registrar. Les informations concernant l'utilisateur et son adresse actuelle sont enregistrées par Registrar sur un serveur qui est utilisé par d'autres proxys, afin de trouver l'utilisateur.
Prise en charge T.38 FAX	Uniquement pour **hybird 300** / **hybird 600** Indiquez si vous voulez transmettre des documents FAX via Voice over IP avec la norme T.38. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut. Si cette fonction est désactivée, les documents FAX sont transmis avec G.711.
Remplacement du préfixe du numéro entrant	Si, en cas d'appels entrants, les numéros d'appel modifiés dans le système sont transmis, saisissez dans la première zone de texte la suite de chiffres du numéro d'appel entrant devant être remplacée par la suite de chiffres entrée dans la deuxième zone de texte.

4.1.2 Emplacements

Le menu **VoIP**->**Paramètres**->**Emplacements** permet de configurer les emplacements des abonnés VoIP configurés sur votre système et de définir la gestion de bande passante pour le trafic VoIP.

Certains emplacements peuvent être configurés à des fins d'utilisation de la gestion de bande passante. Un emplacement est identifié à l'aide de son adresse IP ou DynDNS fixe, ou de l'interface à laquelle l'appareil est connecté. La bande passante VoIP (Upstream et Downstream) disponible peut être configurée pour chaque emplacement.

Champs du menu Comportement d'enregistrement pour participant VoIP sans emplacement défini

Champ	Description
Comportement par défaut	Déterminez la procédure que le système doit suivre lors de l'enregistrement d'abonnés VoIP pour lesquels aucun emplacement n'a été défini. Valeurs possibles : • *Enregistrement seulement dans des réseaux privés* (valeur par défaut) : l'abonné VoIP n'est enregistré que lorsqu'il se trouve sur le réseau privé. • *Pas d'enregistrement* : l'abonné VoIP n'est jamais enregistré. • *Enregistrement illimité*: l'abonné VoIP est toujours enregistré.

4.1.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **VoIP**->**Paramètres**->**Emplacements**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez la description de l'entrée.
Emplacement conte-	Vous pouvez structurer les emplacements SIP selon

Champ	Description
nant (parent)	l'arborescence de votre choix. Déterminez ici quel emplacement SIP déjà défini pour l'emplacement SIP à configurer ici constitue le nœud supérieur de la structure arborescente.
Type	Indiquez si l'emplacement doit être défini à l'aide d'adresses IP/de noms DNS ou d'interfaces. Valeurs possibles : • *Adresses* (valeur par défaut) : l'emplacement SIP est défini via des adresses IP ou des noms DNS. • *Interfaces*: L'emplacement SIP est défini via les interfaces disponibles.
Adresses	Uniquement pour **Type** = *Adresses* Saisissez les adresses IP des appareils aux emplacements SIP. Cliquez sur **Ajouter** pour configurer de nouvelles adresses. Saisissez l'adresse IP ou le nom DNS de votre choix sous **Adresse IP/ Nom DNS**. Saisissez également le **Masque réseau** requis.
Interfaces	Uniquement pour **Type** = *Interfaces* Saisissez les interfaces auxquelles les appareils d'un emplacement SIP sont connectés. Cliquez sur **Ajouter** pour sélectionner de nouvelles interfaces. Sélectionnez l'interface souhaitée sous **Interface**.
Limitation de la bande passante en montée	Déterminez si la bande passante Upstream doit être limitée. Sélectionnez *Activé* pour réduire la bande passante. La fonction est désactivée par défaut.
Bande passante montante maximale	Saisissez le débit de données Upstream maximal en kbits/s.
Limitation de la bande	Déterminez si la bande passante Downstream doit être limitée.

Champ	Description
passante en descente	Sélectionnez *Activé* pour réduire la bande passante. La fonction est désactivée par défaut.
Bande passante maximale en descente	Saisissez le débit de données Downstream maximal en kbits/s.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Paramètres DSCP pour données RTP	Sélectionnez le type de service pour les données RTP (TOS, Type of Service). Valeurs possibles : • *Valeur binaire DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire, 6 bits). • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au format binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63. • *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F.

4.1.3 Profils Codec

Le menu **VoIP**->**Paramètres**->**Profils Codec** permet de définir différents profils Codec pour influencer la qualité sonore et configurer certaines données en fonction du fournisseur.

Lors de la configuration des codecs, tenez compte du fait que la qualité sonore dépend de

la bande passante et que le nombre de communications simultanées est ainsi limité. Le dispositif doit en outre prendre en charge la sélection de codecs correspondante.

4.1.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **VoIP**->**Paramètres**->**Profils Codec**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description pour l'entrée.
Ordre Codec	Indiquez dans quel ordre les codecs doivent être proposés par le système. Si le premier codec ne peut pas être utilisé, le système tentera d'utiliser le deuxième, et ainsi de suite. Valeurs possibles : • *Par défaut* (valeur par défaut) : si possible, le codec placé en première position dans le menu est utilisé. • *Qualité* : les codecs sont triés en fonction de la qualité. si possible, le codec de la meilleure qualité est utilisé. • *Bande passante faible* : les codecs sont triés en fonction de la bande passante nécessaire. Si possible, le codec qui nécessite la bande passante la plus faible est utilisé. • *Bande passante élevée* : les codecs sont triés en fonction de la bande passante nécessaire. Si possible, le codec qui nécessite la bande passante la plus élevée est utilisé.
G.711 uLaw	Uniquement pour **Ordre Codec** non défini sur *Par défaut* Codec RNIS d'après la norme américaine. G.711 uLaw comprend la plage de fréquences allant de 300 à 3 400 Hz avec une fréquence d'échantillonnage de 8 kHz et atteint, pour une vitesse de transfert de données de 64 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 4,4. Ce codec audio utilise la méthode de quantification µlaw.

Champ	Description
G.711 aLaw	Uniquement pour **Ordre Codec** non défini sur *Par défaut* Codec RNIS d'après la norme européenne G.711 aLaw comprend la plage de fréquences allant de 300 à 3 400 Hz avec une fréquence d'échantillonnage de 8 kHz, et atteint, pour une vitesse de transfert de données de 64 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 4,4. Ce codec audio utilise la méthode de quantification alaw.
G.722	Uniquement pour **Ordre Codec** non défini sur *Par défaut* G.722 comprend la plage de fréquences allant de 50 Hz à 7 000 Hz avec une fréquence d'échantillonnage de 16 kHz, et atteint, pour une vitesse de transfert de données de 64 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 4,5.
G.729	Uniquement pour **Ordre Codec** non défini sur *Par défaut* G0,729 comprend la plage de fréquences allant de 300 Hz à 2 400 Hz avec une fréquence d'échantillonnage de 8 kHz, et atteint, pour une vitesse de transfert de données de 8 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 3,9.
G.726 (16 Kbits/s)	Uniquement pour **Ordre Codec** non défini sur *Par défaut* G.726 (16 kbit/s) comprend la plage de fréquences allant de 200 Hz à 3 400 Hz avec une fréquence d'échantillonnage de 8 kHz, et atteint, pour une vitesse de transfert de données de 16 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 3,7.
G.726 (24 Kbits/s)	Uniquement pour **Ordre Codec** non défini sur *Par défaut* G.726 (24 kbit/s) comprend la plage de fréquences allant de 200 Hz à 3 400 Hz avec une fréquence d'échantillonnage de 8 kHz, et atteint, pour une vitesse de transfert de données de 24 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 3,8.
G.726 (32 Kbits/s)	Uniquement pour **Ordre Codec** non défini sur *Par défaut*

Champ	Description
	G.726 (32 kbit/s) comprend la plage de fréquences allant de 200 Hz à 3 400 Hz avec une fréquence d'échantillonnage de 8 kHz, et atteint, pour une vitesse de transfert de données de 32 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 3,9.
G.726 (40 Kbits/s)	Uniquement pour **Ordre Codec** non défini sur *Par défaut* G.726 (40 kbit/s) comprend la plage de fréquences allant de 200 Hz à 3 400 Hz avec une fréquence d'échantillonnage de 8 kHz, et atteint, pour une vitesse de transfert de données de 40 kbit/s, une note d'opinion moyenne (mesure de la qualité sonore) de 4,2.
DTMF	Uniquement pour **Ordre Codec** non défini sur *Par défaut* Indiquez si le codec DTMF Outband doit être utilisé. Le système tente d'abord d'utiliser la RFC 2833. Si le dispositif n'est pas compatible pas cette norme, il utilise SIP Info. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Paramètres Codec G.726	Uniquement pour **Ordre Codec** non défini sur *Par défaut* Sélectionnez le procédé de codage pour le codec G.726. Valeurs possibles : • *I.366* • *RFC3551 / X.420*

4.1.4 Options

Le menu **VoIP**->**Paramètres**->**Options** permet d'accéder aux paramètres généraux pour VoIP.

Le menu **VoIP**->**Paramètres**->**Options** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Port RTP	Saisissez le port via lequel les données RTP doivent être transmises. La valeur définie par défaut est *10000*.
Horloge d'enregistrement de l'appareil terminal	Saisissez ici, en secondes, la valeur par défaut du délai avant l'écoulement duquel les clients SIP doivent se réenregistrer afin que la connexion ne soit pas automatiquement interrompue. La valeur définie par défaut est *60*.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Paramètres DSCP pour données SIP	Sélectionnez le type de service pour les données SIP (TOS, Type of Service). Valeurs possibles : • *Valeur binaire DSCP* (valeur par défaut) : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire, 6 bits). La valeur par défaut est *101110*. • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au format binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63. • *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F.

Chapitre 5 Numérotation

5.1 Connexions externes

Votre système est un appareil de télécommunication servant au raccordement à Euro-ISDN (DSS1) et à Internet :

Interfaces RNIS (S0): Selon l'extension des modules, le système propose des interfaces RNIS externes pouvant être configurées pour un raccord à la connexion RNIS de l'exploitant du réseau. En fonction de l'extension des modules, plusieurs interfaces RNIS peuvent être configurées au choix en tant que connexion RNIS interne ou externe.

Note

Si vous attribuez un nom aux connexions dans ces réglages, celui-ci n'est pas utilisé dans la configuration ultérieure. Il ne sert qu'à la description de la connexion.

5.1.1 Connexions

Dans le menu **Numérotation**->**Connexions externes**->**Connexions**, vous pouvez configurer les connexions externes de votre système.

5.1.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau**pour créer de nouvelles connexions.

Le menu **Numérotation**->**Connexions externes**->**Connexions**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Vous pouvez saisir une description pour la connexion sélectionnée.
Type de connexion	Affiche le type de connexion configuré.

Champ	Description
	Valeurs possibles : • *Connexion point-à-multipoint* (valeur par défaut) • *Connexion de l'installation* • *FXO*
Port	Uniquement pour **Type de connexion** = *Connexion multi-appareils* Sélectionnez la description du port auquel cette connexion externe est raccordée.
Ports	Uniquement pour **Type de connexion** = *Connexion de l'installation* ou **Type de connexion** = *FXO* Sélectionnez la description du port auquel cette connexion externe est raccordée. Toutes les interfaces RNIS extérieures libres sont disponibles. Avec le bouton **Ajouter**, sélectionnez des ports additionnels, par exemple pour configurer un raccordement groupé.

Champs du menu Paramètres pour numéro d'appel sortant

Champ	Description
Numéro d'appel sortant	Sélectionnez la signalisation souhaitée pour les appels vers l'extérieur. Valeurs possibles : • *Standard* (valeur par défaut) • *Numéro d'appel global pour CLIP-No-Screening* • *Numéro d'appel personnel pour CLIP-No-Screening* • *DDI fixe vers externe*
Numéro d'appel global pour CLIP-No-Screening	Uniquement pour **Numéro d'appel sortant** = *Numéro d'appel global pour CLIP-No-Screening* Ici, vous pouvez saisir un numéro d'appel visible par les personnes appelées dans le cadre de communications vers l'extérieur.

Champ	Description
	Ce numéro d'appel n'est pas vérifié.
Afficher le numéro d'appel de l'interlocuteur distant	Uniquement pour **Numéro d'appel sortant** = *Numéro d'appel global pour CLIP-No-Screening* et *Numéro d'appel personnel pour CLIP-No-Screening* Vous pouvez afficher le numéro d'appel d'un interlocuteur externe, dans la mesure où il est signalé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Afficher le numéro d'appel fixe pour les communications sortantes	Uniquement pour **Numéro d'appel sortant** = *DDI fixe vers externe* Pour tous les appels vers l'extérieur, vous pouvez faire afficher un numéro fixe, par exemple, celui de votre central.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Type de numéro d'appel	Sélectionnez le type de numéro pour appels sortants. Valeurs possibles : • *Réglage système* : le paramètre par défaut (réglage du pays) du système est utilisé. • *Inconnu* : Sélectionnez ce réglage lorsque le type de numéro d'appel « Inconnu » est à signaler. • *Subscriber*: il s'agit d'un numéro de poste. • *National* : il s'agit d'un numéro d'appel national (indicatif régional + numéro de poste).
Arrêt dans le système	Indiquez si un appel doit être placé en attente dans le système sans interrompre la communication. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

5.1.2 Numéros d'appel

Dans le menu **Numérotation**->**Connexions externes**->**Numéros d'appel**, vous attribuez les numéros d'appel externes et le nom affiché sur l'écran d'un téléphone système aux connexions externes que vous avez définies.

Un raccordement externe peut être configuré en tant que connexion point-à-multipoint ou point-à-point ; ici la description de la connexion est définie. Le nom de port préconisé est alors attribué à cette connexion. Le nom de port (**Description**) peut être défini sous **Interfaces physiques**->**Ports RNIS**->**RNIS externe** pour la connexion du module.

Numéros d'appel externes à la connexion point-à-point

Avec une connexion point-à-point, vous recevez un numéro d'appel système avec un plan de numérotation à 1, 2, 3, ou 4 chiffres. Ce plan de numérotation compose les numéros directs pour la connexion point-à-point. En commandant plusieurs raccordements point-à-point vous pouvez augmenter le nombre de numérotations directes, ou bien vous recevez un numéro d'appel système supplémentaire avec plan de numérotation dédié.

Avec la connexion point-à-point, les appels externes sont signalés à l'abonné dont le numéro d'appel interne attribué correspond au numéro d'appel direct composé. Vous pouvez configurer les numéros d'appel internes à joindre directement par la numérotation directe du plan de numérotation en tant que **Numéro d'Appel Interne** dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Ajouter**->**Numéros d'appel**->**Numéros d'appel internes**.

Exemple : Vous avez une connexion point-à-point avec le numéro système *1234* et numéros d'appel directs de *0* à *30*. Un appel au *1234-22* est normalement signalé à l'abonné interne par le numéro d'appel *22*. Cependant, si vous entrez la numérotation directe *22* dans cette liste, vous pouvez définir que les appels au *1234-22* soient signalés à l'abonné interne au numéro d'appel *321*.

Numéros d'appel externes au raccordement point-à-multipoint

Avec un raccordement point-à-multipoint, vous pouvez commander jusqu'à 10 numéros d'appel (numéros d'abonné multiple) par connexion RNIS. Ces numéros d'abonné multiple sont les numéros d'appel externes de vos raccordements RNIS. La définition des numéros d'appel internes est effectuée sous **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Ajouter**->**Numéros d'appel**.

5.1.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Utilisez le bouton **Nouveau** pour créer de nouveaux numéros d'appel.

Le menu **Numérotation**->**Connexions externes**->**Numéros d'appel**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Connexion externe	Sélectionnez la connexion définie dans **Numérotation**->**Connexions externes**->**Connexions** pour laquelle vous désirez effectuer la configuration de numéro d'appel.
Type de numéro d'appel	Selon la nature du raccordement, sélectionnez le type de numéro d'appel à définir. Valeurs possibles : • *Numéro d'appel unique (MSN)* : uniquement pour connexions point-à-multipoint. • *Numéro d'appel Connexion de l'installation* : uniquement pour les connexions d'installations. • *Exception numérotation directe (P-P)* : uniquement pour les connexions d'installations. • *Connexion de l'installation MSN supplémentaire* : uniquement pour les connexions d'installations.
Nom affiché	De manière générale, vous saisissez le nom qui doit s'afficher sur l'écran du téléphone système appelé pour ce numéro d'appel. Pour **Type de numéro d'appel** = *Numéro d'appel Connexion de l'installation* ce champ affiche le nom de la connexion.
Numéro d'appel unique (MSN)	Ici, saisissez le numéro d'abonné multiple pour une connexion point-à-multipoint.
Numéro d'appel Connexion de	Ici, saisissez le numéro d'abonné multiple pour une connexion point-à-point (sans numéro d'appel directe).

Champ	Description
l'installation	
Exception numérotation directe (P-P)	Ici, saisissez l'exception numérotation directe pour une connexion point-à-point. Remarque : Saisissez ici uniquement la numérotation directe selon votre plan de numérotation à transmettre à différents numéros internes directs. La numérotation directe à la connexion point-à-point s'effectue toujours vers l'abonné dont le numéro d'appel a été composé ; par exemple, l'abonné interne a le numéro d'appel *16*. Si cet abonné est appelé de l'extérieur avec *1234567-16*, l'appel est signalé à son téléphone. Cependant, si avec la numérotation directe *16* vous désirez appeler un abonné avec le numéro d'appel *888*, saisissez le *888* comme exception de numéro d'appel. Puis, dans **Affectation des appels**, vous attribuez à l'abonné au numéro d'appel *16* l'exception de numéro d'appel. Vous pouvez ensuite effectuer des réglages supplémentaires dans **Affectation des appels**.
Connexion de l'installation MSN supplémentaire	Ici, saisissez un numéro d'abonné multiple supplémentaire pour une connexion point-à-point. Avec certains fournisseurs, il est possible de transmettre encore un numéro d'appel point-à-multipoint sur une connexion point-à-point en parallèle au numéro d'appel direct, par exemple un numéro de fax préexistant à l'établissement d'une connexion point-à-point ou l'ancien numéro d'abonné multiple.

5.1.3 Groupage

Au menu **Numérotation**->**Connexions externes**->**Groupage**, vous pouvez réunir diverses connexions externes et les placer individuellement à la disposition des utilisateurs.

Vous désirez attribuer certaines connexions externes aux abonnés internes pour les appels sortants. Vous pouvez réunir ces connexion externes en groupages et les mettre à la disposition des abonnés pour les appels sortants. Ainsi, tous les abonnés commencent la numérotation pour un appel externe avec le même indicatif, mais ne peuvent établir une connexion que via le groupage qui leur a été attribué.

Les raccordements externes de votre système peuvent être réunis en groupages. Ici, vous pouvez créer jusqu'à 99 groupages (01 - 99). Le code pour la répartition en groupage peut être modifié (menu **Codes modifiables**)

Lors de l'initiation d'un appel externe via le code de groupage, le groupage attribué à l'abonné est utilisé dans l'établissement de la connexion.

5.1.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour créer un nouveau groupage.

Le menu **Numérotation**->**Connexions externes**->**Groupage**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'entrée.
Ordre dans le groupage	Sélectionnez les connexions externes souhaitées pour un groupage. L'ordre de la numérotation vers l'externe correspond au déroulement des connexions externes dans cette liste. Vous désirez attribuer certaines connexions externes aux abonnés internes de votre système pour les appels sortants. Vous pouvez réunir les connexions externes en groupages et les mettre à la disposition des abonnés pour les appels sortants. Ainsi, tous les abonnés commencent la numérotation pour un appel externe avec le même code de groupage, mais ne peuvent établir une connexion que via le groupage qui leur a été attribué.

5.1.4 X.31

Transfert de données en mode paquet (X.31)

Afin d'améliorer la qualité de service pour vos clients, vous désirez leur proposer l'option de paiement en monnaie scripturale par carte bleue ou carte de crédit, ou bien enregistrer des données d'achat pour une carte client. A cet effet, vous raccordez à votre système un appareil qui transmet les données des clients/cartes de crédit vers une centrale.

Vous pouvez raccorder un terminal de traitement des données fonctionnant selon la norme de transmission X.31 (transmission des données sur canal D) aux connexions RNIS internes du système. Il s'agit, par exemple,de terminaux de caisse, de DAB ou d'appareils pour cartes client.

Pour l'utilisation de cette fonctionnalité, des TEI‘s (Terminal Endpoint Identifier) vous sont communiqués; vous les attribuez aux connexions individuelles lors de la configuration du système. Ces TEI’s permettent un adressage supplémentaire de ces terminaux.

Note

Cette fonctionnalité est uniquement disponible si la fonctionnalité **X.31** a été commandée auprès de l'opérateur du réseau et que vous exploitez un périphérique correspondant sur cette connexion. Pour l'utilisation, veuillez vous référer aux manuels des terminaux en question.

5.1.4.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer d'autres applications X.31.

Le menu **Numérotation**->**Connexions externes**->**X.31**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Sélectionner interface	Sélectionnez l'interface externe via lequel vous joignez l'opérateur du réseau qui met la fonctionnalité X.31 à votre disposition.
Terminal Endpoint Identifier (TEI)	Ici, sélectionnez la valeur TEI (Terminal Endpoint Identifier) que vous avez reçue de votre opérateur réseau. Les TEI’s permettent un adressage supplémentaire de ces terminaux. Les valeurs possibles sont comprises entre *00* et *63*. La valeur par défaut est *00*.
Affectation interne	Sélectionnez l'interface RNIS interne auquel votre périphérique de traitement des données fonctionnant selon la norme de transmission X.31 (transmission des données sur canal D) est connecté.

5.2 Paramètres de l'utilisateur

Dans ce menu, vous configurez et administrez les utilisateurs de votre système. Les utilisateurs sont repartis en classes d'autorisation auxquelles sont attribuées les lignes externes désirées et qui peuvent utiliser les fonctionnalités selon les besoins. L'utilisateur auquel a été attribué une classe d'autorisation reçoit un numéro d'appel interne et certaines autorisations. Une classe d'autorisation par défaut (Default CoS) est prédéfinie ; elle est automatiquement attribuée aux nouveaux utilisateurs.

Une fois que l'attribution des fonctions et des autorisations à tel ou tels utilisateur(s) est définie dans les paramètres utilisateur, l'autorisation des paramètres utilisateur est attribuée à un terminal dans le menu **Appareils terminaux**. Ainsi est rendue possible la configuration du réglage de plusieurs terminaux via une classe d'autorisation, par exemple, un réglage utilisateur *Chef*, un réglage utilisateur *Chef de service* et un réglage utilisateur *Responsable du dossier*. A présent, il ne reste plus qu'à attribuer aux utilisateurs correspondants l'une de ces **Classe d'autorisation**.

5.2.1 Utilisateur

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur** vous configurez les utilisateurs de votre système, leurs classe, et vous leurs attribuez des numéros d'appel internes et externes.

Une vue d'ensemble des utilisateurs déjà créés s'affiche Dans la colonne **Nom**, les entrées sont classées par ordre alphabétique. Vous pouvez cliquer sur le titre de toute autre colonne et trier les entrées dans l'ordre croissant ou décroissant.

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des utilisateurs.

5.2.1.1 Configuration de base

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Configuration de base**, vous saisissez les informations de base sur l'utilisateur.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Configuration de base** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Nom	Saisissez le nom de l'utilisateur.

Champ	Description
	Ce nom est indiqué dans le répertoire téléphonique si vous avez saisi un numéro d'appel dans **Numéro de mobile Numéro d'appel privé** et l'avez autorisé pour le répertoire. Le nom est indiqué avec l'indicatif (M) pour téléphonie mobile et (H) pour numéro personnel à l'écran du téléphone système.
Description	Saisissez les informations supplémentaires sur l'utilisateur.

Champs du menu Numéros d'appels externes

Champ	Description
Numéro de mobile	Saisissez un numéro d'appel pour joindre l'utilisateur par téléphone portable. Déterminez également si ce numéro d'appel doit s'afficher sur l'écran du téléphone système, afin de pouvoir être sélectionné dans le répertoire téléphonique du système via le téléphone système (option **Accès via le téléphone système**).
Numéro d'appel privé	Saisissez un numéro d'appel pour joindre l'utilisateur par numéro d'appel personnel. Déterminez également si ce numéro d'appel doit s'afficher sur l'écran du téléphone système, afin de pouvoir être sélectionné dans le répertoire téléphonique du système via le téléphone système (option **Accès via le téléphone système**).
Adresse e-mail	Saisissez l'adresse email de l'utilisateur.

Champs du menu Classe d'autorisation

Champ	Description
Par défaut	Sélectionnez la classe d'autorisation = CoS (Class of Service). La définition de la classe d'autorisation ainsi que la création de classes d'autorisation s'effectuent sous **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**. Ce paramètre permet uniquement d'effectuer la sélection. Valeurs possibles : • *Default CoS* (valeur par défaut) • *Non autorisé* : aucune classe d'autorisation • *<Classe d'autorisation>*

Champ	Description
Optionnel	Sélectionnez une classe d'autorisation facultative. Cette CoS est nécessaire dans les paramètres du calendrier. La définition de la classe d'autorisation ainsi que la création de classes d'autorisation s'effectuent sous **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**. Ce paramètre permet uniquement d'effectuer la sélection. Valeurs possibles : • *Default CoS* (valeur par défaut) • *Non autorisé* : aucune classe d'autorisation • *<Classe d'autorisation>*
Nuit	Sélectionnez la classe d'autorisation pour le service de nuit. Cette CoS est nécessaire dans les paramètres du calendrier. La définition de la classe d'autorisation ainsi que la création de classes d'autorisation s'effectuent sous **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**. Ce paramètre permet uniquement d'effectuer la sélection. Valeurs possibles : • *Default CoS* (valeur par défaut) • *Non autorisé* : aucune classe d'autorisation • *<Classe d'autorisation>*

Champs du menu Autres options

Champ	Description
Occupé par occupé (Busy on Busy)	Sélectionnez si la fonctionnalité « Busy on Busy » doit être activée pour cet utilisateur. Si un utilisateur, pour lequel plusieurs numéros de téléphone sont définis, est en communication, vous pouvez déterminer si les autres appels destinés à cet utilisateur doivent être signalés. Si la fonctionnalité « Busy on Busy » est configurée pour cet utilisateur, les autres appelants reçoivent un signal **Occupé** lorsque l'utilisateur appelle l'un de ses numéros. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

5.2.1.2 Numéros d'appel

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Numéros d'appel**, vous pouvez saisir les numéros d'appel internes qui seront ensuite attribués aux terminaux. Selon le type, un ou plusieurs numéros d'appel pourront alors être attribués à chaque terminal.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Numéros d'appel** se compose des champs suivants :

Champs du menu Numéros d'appel internes

Champ	Description
Numéros d'appel internes	Saisissez les numéros d'appel internes pour l'utilisateur, ainsi que la description à afficher à l'écran des téléphones système (**Description affichée**). Sélectionnez également si ce numéro interne doit s'afficher dans le **Répertoire téléphonique du système**, et si le LED face à la touche de fonction correspondante doit s'allumer (**Champ lampe occupé**). Les fonctions sont activées par défaut. Avec **Ajouter**, ajoutez de nouveaux **Numéros d'appel internes**.

5.2.1.3 Numéro d'appel sortant

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Numéro d'appel sortant**, vous sélectionnez les numéros d'appel sortants pour l'utilisateur.

Si, lors d'un appel sortant, l'interlocuteur distant ne doit pas connaître le numéro d'appel attribué au propre raccordement, l'un des numéros d'appel existants peut être sélectionné ici pour affichage. Si aucun numéro d'appel n'a été sélectionné, le système n'envoie aucun numéro d'appel au fournisseur.

Champs dans la liste Numéro d'appel sortant

Champ	Description
Numéro d'appel interne	Permet d'afficher les numéros d'appel internes configurés pour l'utilisateur.
Description affichée	Permet d'afficher, pour chaque numéro de téléphone interne, la description configurée pour l'affichage sur l'écran des télé-

Champ	Description
	phones système.
Numéro d'appel sortant	Sélectionnez la signalisation souhaitée pour les appels vers l'extérieur. Valeurs possibles : • *Signaux DDI propres par défaut* : Votre propre numérotation directe est utilisée comme **Numéro d'appel sortant**. Cette option est disponible pour une connexion d'installation ou un fournisseur SIP avec numérotation directe. • *Par défaut* : Aucun **Numéro d'appel sortant** n'est transmis. Dans ce cas, le central utilise le numéro d'appel principal de la connexion. • *<Numéro d'appel fixe>* : Pour une interface FXO, le numéro d'appel configuré est déjà attribué en tant que **Numéro d'appel sortant**et s'affiche. • *<Numéro d'appel>* : S'il existe plusieurs numéros configurés, vous pouvez sélectionner un numéro d'appel que vous désirez utiliser en tant que **Numéro d'appel sortant**.

Sélectionnez le symbole afin de définir pour chaque numéro d'appel interne (indiqué dans la table avec **Numéro d'appel interne** et **Description affichée**) quel numéro d'appel indiquer lors d'appels sortants. Ici, pour chaque connexion externe configurée, vous choisissez l'un des numéros configurés correspondants.

Si plusieurs connexions externes sont configurées, vous pouvez définir comment procéder avec les appels sortants. L'ordre des entrées détermine l'ordre de sélection parmi les autres lignes attribuées en cas de ligne externe occupée.

Le **Numéro d'appel sortant** configuré peut être individuellement caché pour chaque ligne vers l'extérieur ; pour cela, cochez **Masquer le numéro** à la ligne correspondante.

Si vous désirez déplacer une entrée sur la liste affichée, sélectionnez le symbole à la ligne correspondante. Une nouvelle fenêtre s'ouvre.

L'entrée sélectionné est affichée dans **Connexion externe**; ici, par exemple, *ISDN_1*.

Pour déplacer l'entrée sélectionnée, procédez comme suit :

(1) Dans **Déplacer** sélectionnez dans la liste l'entrée par rapport à laquelle vous désirez

déplacer l'entrée sélectionnée, ici, par exemple, *1.SIP-Provider_1*.

(2) Choisissez d'ordonner l'entrée *au dessus* ou *au dessous* de l'entrée sélectionnée dans la liste, ici, par exemple, *au dessus*.

(3) Sélectionnez **Appliquer**.
Les entrées sont affichées dans l'ordre modifié.

(4) Si la liste comprend plus de deux entrées, vous déplacez éventuellement d'autres entrées.

L'ordre configuré ici écrase le réglage attribué par la classe d'autorisation. La classe d'autorisation attribuée continue cependant de déterminer si un utilisateur a accès à une connexion externe spécifique.

5.2.1.4 Rejet optionnel

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Rejet optionnel** vous pouvez attribuer a chacun des numéros d'appel affichés d'un abonné une **Application de rejet** et un **Variante active (jour)**.

Ici, par exemple, vous pouvez paramétrer vers quel collègue transférer vos appels lorsque vous êtes en réunion, ou si le central prend vos appels durant votre pause déjeuner.

Champs du menu Rejet optionnel

Champ	Description
Numéro d'appel interne	Permet d'afficher les numéros d'appel internes configurés pour l'utilisateur.
Description affichée	Permet d'afficher, pour chaque numéro de téléphone interne, la description configurée pour l'affichage sur l'écran des téléphones système.
Application du rejet	Sélectionnez dans la liste déroulante l'application de rejet que vous désirez attribuer au numéro interne. Vous pouvez choisir parmi les applications de rejet que vous avez configurées dans le menu **Applications**->**Rejet**->**Applications du rejet**->**Nouveau** avec **Type d'application de rejet** = *Abonné interne*. Valeurs possibles : • *aucun* • <Application de rejet>

Champ	Description
Variante active (jour)	Sélectionnez la variante de l'application de rejet (qui doit normalement être activée). Si une commutation des variantes est définie via le calendrier, ce paramètre est à nouveau modifié en temps utile. Valeurs possibles : • *Variante 1* • *Variante 2* • *Variante 3* • *Variante 4*

5.2.1.5 Autorisations

Dans le menu**Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Autorisations**, vous pouvez permettre à l'utilisateur d'effectuer certains réglages lui-même via la configuration HTML. Pour cela, le nom d'utilisateur et le mot de passe doivent être entrés dans configuration HTML utilisateur et l'accès personnel autorisé. Après la déconnexion, suivant la saisie de ce nom d'utilisateur et du mot de passe, l'on peut afficher et modifier les réglages correspondants.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Autorisations** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Mot de passe pour enregistrement téléphonique IP	Saisissez le mot de passe avec lequel un téléphone IP de l'utilisateur doit se connecter au système. Le mot de passe peut rester libre lorsque les téléphones IP doivent s'enregistrer mais pas s'authentifier.
PIN pour accès par téléphone	Ici, vous pouvez modifier le PIN pour le répondeur personnel (Voice Mailbox) de l'utilisateur. La valeur par défaut est *néant*.

Champs du menu Configuration HTML utilisateur

Champ	Description
Accès personnel	Sélectionnez si cet utilisateur doit pouvoir accéder à une interface utilisateur (accès utilisateur) où effectuer des entrées ou

Champ	Description
	des réglages propres. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Nom de l'utilisateur	Activé uniquement pour **Accès personnel**. Saisissez un nom pour cet utilisateur. Celui-ci est requis pour se connecter à l'interface utilisateur.
Mot de passe	Activé uniquement pour **Accès personnel**. Saisissez un mot de passe pour cet utilisateur. Celui-ci est requis pour se connecter à l'interface utilisateur.

Call Through

Call Through désigne la connexion entrante au système via un branchement externe, puis le transfert de l'appel sortant du système via un autre branchement.

Note

Dans les paquets de connexion, un paquet est généré pour la connexion entrante, un autre pour la connexion sortante.

Champs du menu Autres options

Champ	Description
Call Through	Indiquez si Call Through doit être autorisé pour cet utilisateur. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Si vous activez la fonctionnalité, vous devez sélectionner dans **Utiliser les paramètres du numéro d'appel** à partir de quel numéro interne les lignes externes autorisées et les variantes d'appel doivent être autorisées pour Call Through.

5.2.2 Classes d'autorisation

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation** (CoS) les fonctionnalités et caractéristiques pour les réglages utilisateur sont définies. Ces classes d'autorisation peuvent alors être attribuées aux utilisateurs individuels dans les réglages utilisateur (groupes d'utilisateurs).

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer d'autres classes d'autorisation. Par défaut, la classe d'autorisation *CoS par défaut* est configurée.

5.2.2.1 Configuration de base

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Configuration de base** sont définis les paramétrages de base ainsi que le nom de la nouvelle classe d'autorisation Vous pouvez trouver la classe d'autorisation par le nom.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Configuration de base** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'entrée.

Champs du menu Autorisation de numérotation

Champ	Description
Autorisation de numérotation	Sélectionnez l'autorisation de numérotation pour la classe d'autorisation. L'autorisation de numérotation détermine quels appels (internes, externes,...) peuvent être effectués. Le système distingue plusieurs niveaux d'autorisation. Valeurs possibles : • *Illimité* : les téléphones disposent d'autorisations illimitées quant à la numérotation et peuvent établir eux-mêmes toutes les connexions. • *National* : les téléphones peuvent établir eux-mêmes toutes les communications, à l'exception des communica-

Champ	Description
	tions internationales. Si un numéro d'appel commence par le code de numérotation internationale, il ne peut pas être sélectionné. • *Entrant* : les téléphones sont accessibles pour les communications externes entrantes, mais ne peuvent pas établir eux-mêmes de communications externes. Les communications internes sont possibles. • *Région* : les téléphones ne peuvent pas établir de communications nationales et internationales. Pour cette autorisation de numérotation, 10 numéros d'exception peuvent être configurés, via lesquels il est possible d'effectuer une numérotation nationale ou internationale. Un numéro d'exception peut être composé de numéros d'appel entiers ou de parties d'un numéro d'appel (p. ex. les premiers chiffres). • *Lieu* : les téléphones peuvent établir des communications locales. Il est impossible d'établir des communications nationales et internationales. • *Interne* : les communications externes entrantes et sortantes ne sont pas autorisées sur ces téléphones. Seules les communications internes sont autorisées.
Ligne extérieure automatique	Ce réglage détermine si l'accès automatique au réseau public est configuré pour.la classe d'autorisation. Avec l'accès automatique au réseau public, les utilisateurs de cette classe d'autorisation entendent la tonalité de numérotation après avoir décroché le combiné et sont immédiatement en mesure de numéroter vers l'extérieur. Pour un appel interne, l'utilisateur doit d'abord appuyer sur la touche étoile après avoir décroché le combiné.
Occupation de la ligne avec indicatif	Sélectionnez les connexions via lesquelles les appels sortants de ces téléphones seront transférés vers l'extérieur. L'ordre de l'entrée détermine l'ordre de sélection parmi les autres lignes attribuées en cas de ligne externe occupée.
Autoriser groupage manuel	Outre l'occupation générale de la ligne, un téléphone permet également un groupage ciblé. Dans ce cas, une connexion externe induit un groupage ciblé grâce au code correspondant, et non grâce à la numérotation de l'indicatif. Pour pouvoir effectuer un groupage ciblé, la classe

Champ	Description
	d'autorisation doit disposer de l'autorisation adéquate. Cette autorisation peut également comprendre des groupages, que la classe d'autorisation ne peut pas autoriser autrement. Si un téléphone ne dispose pas de l'autorisation de groupage ciblé ou si le groupage sélectionné est occupé, la sonnerie « occupé » retentit après la numérotation du code. Si la l'**accès public automatique** est configuré pour une classe d'autorisation, les utilisateurs de cette classe d'autorisation doivent appuyer sur la touche étoile avant un groupage ciblé, puis initier la numérotation externe à l'aide du code pour groupage. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Puis sélectionnez les groupages pour lesquels le groupage manuel doit être autorisé. Le menu **Numérotation**->**Connexions externes**->**Groupage** permet de configurer les groupages.

Affichage du numéro d'appel

Lorsque vous téléphonez à un correspondant, votre numéro d'appel s'affiche chez lui. Ainsi, votre correspondant est averti que c'est vous qui appelez avant même d'avoir décroché. Si vous ne désirez pas que votre numéro soit communiqué à votre correspondant avant qu'il ne décroche, vous pouvez empêcher l'affichage de votre numéro chez votre correspondant.

Si votre correspondant a configuré un transfert d'appel, vous ne saurez pas sur quel téléphone vous l'avez joint. Dans ce cas, vous pouvez afficher le numéro d'appel sur lequel votre correspondant à fait transférer l'appel. Cependant, votre correspondant a également la possibilité d'empêcher l'affichage de ce numéro d'appel.

L'affichage du numéro d'appel permet de connaître le numéro de l'appelant dès que l'appel est signalé, également sur un téléphone analogique. Ainsi, vous savez qui cherche à vous joindre avant même d'avoir pris l'appel.

Note

La transmission de données CLIP analogiques peut être configurée pour chaque connexion analogique. Pour savoir si vos périphériques analogiques prennent en charge les fonctionnalités « CLIP » et « CLIP off Hook », reportez-vous à leurs manuels respectifs.

Toutes les fonctionnalités décrites ne sont pas comprises dans la connexion RNIS standard. Veuillez vous renseigner auprès de votre opérateur de réseau pour savoir dans quelle mesure les fonctionnalités individuelles pour votre connexion RNIS doivent être commandées séparément.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Autres paramètres

Champ	Description
Contrôle de numérotation	Indiquez si les numéros d'appel entrés au menu **Contrôle d'appel**->**Services sortants**->**Contrôle de numérotation** doivent être bloqués ou autorisés également pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Règles de sélection (ARS)	Sélectionnez si les règles de routage entrées au menu **Contrôle d'appel**->**Règles de sélection** doivent être appliquées également pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Transmettre le numéro d'appel A (CLIP)	Indiquez si le numéro de l'appelant doit être affiché auprès de l'appelé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Transmettre le numéro d'appel B (COLP)	Indiquez si le numéro de l'appelé doit être affiché auprès de l'appelant. Si, par exemple, l'appelé a configuré un transfert d'appel vers

Champ	Description
	un abonné tiers, l'appelant peut afficher le numéro d'appel de destination du transfert d'appel grâce à cette fonctionnalité. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Informations supplémentaires sur l'appel externe	Indiquez les informations qui doivent être affichées sur l'écran pendant un appel. Valeurs possibles : • *Nom de la connexion et du numéro* : L'accès au réseau public et le nom attribué sont successivement affichés. • *Uniquement nom de la connexion* : uniquement le nom de l'accès au réseau public est affiché. • *Uniquement nom du numéro* (valeur par défaut) : Uniquement le nom attribué au numéro d'appel externe est affiché à l'écran. • *aucun* : Aucun affichage à l'écran.

5.2.2.2 Caractéristiques de la prestation

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Caractéristiques de la prestation** des fonctionnalités supplémentaires sont configurées.

Interception d'appels (Pick-Up)

Un appel est signalé chez un collègue qui ne se trouve pas actuellement à son poste de travail. Vous n'avez que deux options pour prendre en charge l'appel. Vous pourriez vous lever et vous déplacer vers le téléphone de votre collègue, ou bien vous transférez l'appel pour votre collègue sur votre téléphone.

Un appel signalé sur un autre téléphone peut être intercepté à l'aide d'un code. L'attribution s'opère via l'option **Groupe Pick-Up** dans le menu **Caractéristiques de la prestation**, qui est alors attribué à l'abonné. Un Pick-Up est possible en cas de valeur égale. L'interception de l'appel n'est pas possible en cas de mise en attente.

Les téléphones système peuvent intercepter les appels avec des touches de fonction programmables. Sur des téléphones système, vous pouvez configurer des touches ligne, des touches poste ou des touches d'équipe.

- Touche ligne : Vous pouvez définir une touche ligne pour une connexion RNIS ou un fournisseur VoIP. La diode lumineuse correspondante à la touche ligne indique l'état de la connexion. La LED brille lorsque les deux canaux B d'une connexion sont occupés, ou lorsque le nombre maximum de connexions simultanées via un fournisseur VoIP est atteint. Si un appel externe est signalé sur un autre téléphone interne, vous pouvez l'intercepter en appuyant sur la touche ligne.
- Touche poste: Vous pouvez définir une touche poste pour un utilisateur du système. La diode lumineuse correspondante à la touche poste indique l'état de l'abonné (appel, communication,...). Si l'abonné interne reçoit un appel, vous pouvez l'intercepter en appuyant sur la touche poste.
- Touche équipe : Une touche équipe est une touche poste ordinaire à laquelle est attribuée le numéro interne d'une équipe. La diode lumineuse correspondante à la touche équipe indique l'état de l'équipe (appel, communication,...). Si l'équipe reçoit un appel, vous pouvez l'intercepter en appuyant sur la touche équipe.

Signal d'appel en attente

Vous désirez, autant que possible, répondre à l'appel de chaque client, même lorsque vous êtes au téléphone. Si un autre appel est signalé à votre téléphone par un signal sonore d'appel en attente ou un message à l'écran, vous pouvez décider avec lequel des deux clients vous entretenir.

Si un abonné interne reçoit un appel alors qu'il est déjà en communication, le signal sonore d'appel en attente se déclenche automatiquement chez lui. Le signal sonore d'appel en attente est possible pour les communications internes comme externes. La communication en attente est signalée chez l'appellé de manière visuelle ou sonore, selon le terminal.

L'appelé peut :

- Rejeter l'appel en attente et poursuivre la communication en cours. L'appelant entend alors une tonalité « occupé ».
- Accepter l'appel en attente et interrompre la communication en cours.
- Accepter l'appel en attente après avoir terminé la communication en cours.
- Ignorer l'appel en attente. Après 30 secondes, l'attente se termine automatiquement et l'appelant entend une tonalité « occupé ».

Appareils terminaux analogiques

L'option appel en attente peut être réglée individuellement pour chaque abonné. Autoriser ou non l'appel en attente peut être paramétré via la configuration ou un code dans la commande.

Les appareils terminaux analogiques entendent le signal d'appel en attente du système.

Le numéro de l'appelant en attente peut être affiché à l'écran du téléphone analogique, si celui-ci dispose de la fonctionnalité correspondante (CLIP off Hook). Chez les terminaux analogiques, « CLIP off Hook » est désactivé dans la configuration de base, mais peut être activé dans la configuration.

Dans le système, on ne peut se mettre simultanément en attente que d'un nombre limité de communications analogiques. Lorsqu'on lance des appels en attente sur des communications analogiques alors que le nombre maximum d'appels en attente est déjà atteint, les appelants en attente suivants entendent la tonalité « occupé ».

Si vous entendez le signal sonore de l'appel en attente pendant une communication, vous pouvez prendre le nouvel appel et transférer l'appel en cours. Un procédé opérationnel vous permet de transférer la communication en cours, tout en acceptant l'appel en attente. Ici s'appliquent les conditions suivantes :

- Chaque numéro d'appel numéroté est pris en charge par le système.
- Après le procédé opérationnel, l'abonné et l'abonné en attente sont immédiatement mis en communication (sans signaux de confirmation).
- Un transfert vers son propre numéro est possible ; l'appel est alors placé en attente.
- Des abonnés destinataires internes comme externes, ainsi que des équipes, peuvent être appelés.
- Si le numéro de destination est erroné ou occupé, l'appel est répété.
- Si l'abonné est libre, l'appel est répété après le délai configuré par l'abonné appelé.
- En cas de transfert vers un numéro d'appel équipe, l'appel n'est pas répété avec un équipe occupée ou injoignable.
- En cas de transfert vers un numéro d'appel équipe, seul la fonctionnalité rappel ponctuel est prise en charge.

Terminaux RNIS

Le paramétrage et l'utilisation de la fonctionnalité appel en attente s'effectue selon les manuels des terminaux respectifs. Les terminaux RNIS utilisent leurs propres tonalités pour signaler l'appel en attente.

Note

L'appel en attente n'est pas possible :

- pour les télé-réunions
- en cas de fonctionnalité silence du téléphone (terminaux analogiques)
- en cas d'annonce

- en cas de surveillance des locaux
- avec des terminaux chez lesquels la fonctionnalité « protection des données » est configurée (ex. fax, modem)
- pendant la numérotation d'un abonné analogique (le combiné est décroché mais la communication n'est pas encore établie)
- en cas de blocage des appels en attente
- lors de la numérotation d'un numéro d'appel équipe. Dans ce cas, il n'y a pas d'appel en attente chez les abonnés équipe analogiques.

Les téléphones RNIS peuvent également transférer un appel en attente vers un autre abonné via la fonctionnalité « Call Deflection ». Une communication en cours est terminée par exemple en raccrochant le combiné. L'appel en attente est alors signalé et peut être accepté, par exemple en décrochant le combiné.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Caractéristiques de la prestation** se compose des champs suivants :

Champs du menu Autorisation

Champ	Description
Groupe Pick-Up	Saisissez le numéro du groupe dans lequel les appels peuvent être interceptés.
Signal appel en attente	Indiquez si l'appel en absence est autorisé pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Utiliser le rejet global	Indiquez si un rejet global est autorisé pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. **Note** La destination de rejet doit se trouver dans un classe d'autorisation sans rejet global.

Champ	Description
Commuter les variantes d'appel manuellement	Indiquez si la commutation manuelle des variantes d'appel est autorisée pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Call Through	Indiquez si Call Through est autorisé pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Interphone

La fonction interphone vous permet d'établir une connexion d'un téléphone système à un autre téléphone système sans que la connexion n'aie besoin d'être activement acceptée par le téléphone système appelé (décrocher le combiné, enclencher main libres/ haut-parleur). La connexion est établie aussitôt que le téléphone système a accepté la connexion interphone. Les téléphones système appelants ainsi que appelés entendent une tonalité de signalement au début de l'appel interphone. La durée de l'appel interphone est limitée à deux minutes. Si, durant cette période, le combiné d'un des téléphones impliqués est décroché, la communication devient un appel normal.

Les téléphones système peuvent initier un appel interphone dans le menu du téléphone système ou par une touche fonction programmée. Si l'appel interphone est lancé via une touche fonction, les messages apparaissant à l'écran du téléphone système sont les mêmes que lors d'une communication normale, et la diode lumineuse de la touche interphone s'allume. Pour mettre fin à l'appel interphone, appuyez à nouveau sur la touche fonction, ou appuyez sur la touche du haut-parleur. Une fois l'appel interphone terminé, la diode lumineuse s'éteint à nouveau.

Si un téléphone ou un téléphone système est destinataire d'un appel interphone, le numéro d'appel de l'appelant est affiché à l'écran. L'appel interphone est annoncé par le haut-parleur à l'aide d'une tonalité de signalement. Pour mettre fin à l'appel interphone, appuyer sur la touche ESC.

Une touche fonction peut également être configurée sur un téléphone système pour bloquer ou autoriser les appels interphone.

Note

Les appels interphone sont automatiquement acceptés par le téléphone appelé par activation de la fonction mains libres, si :

- le téléphone est en veille,
- les appels interphone sont autorisés et
- la fonctionnalité « silence du téléphone » (protection d'appel) n'est pas activée.

Si un appel interphone n'est pas clos par l'un des deux interlocuteurs, la connexion est automatiquement interrompue par le système au bout d'environ 2 minutes.

Annonce

Vous désirez convier vos collègues à une réunion ou à un repas ? Vous pourriez appeler chacun individuellement, ou simplement faire usage de la fonctionnalité annonce. Avec un seul appel, vous contactez tous les téléphones autorisés aux annonces, sans que vos correspondants n'aient même besoin de décrocher.

Attention

Alors que vous vous faites entendre grâce à l'annonce, vous n'entendez pas les éventuels commentaires de vos collègues ou de leurs familles.

La fonction annonce vous permet d'établir une connexion avec un autre téléphone, sans pour autant que cette connexion n'aie besoin d'être activement acceptée par ce dernier (décrocher le combiné, enclencher main libres/haut-parleur). La connexion est établie aussitôt qu'un téléphone a accepté l'annonce. Au début d'une annonce, l'annonceur ainsi que l'abonné appellé entendent un signal de confirmation. La durée d'une annonce n'est pas limitée.

L'annonce est possible pour les téléphones RNIS et analogiques, du moment que ceux-ci prennent en charge la fonctionnalité annonce. Pour savoir si la fonctionnalité est prise en charge, reportez-vous aux manuels utilisateur de vos téléphones.

Les annonces peuvent être autorisées ou bloquées sur les téléphones à l'aide d'un code.

Téléphones système

Les annonces à partir de, et vers, des téléphones système sont possibles. Les téléphones système peuvent initier une annonce dans le menu du téléphone système ou par une

touche fonction programmée. Si l'annonce est lancée via une touche fonction, les messages apparaissant à l'écran de votre téléphone sont les mêmes que lors d'une communication normale, et la diode lumineuse de la touche annonce s'allume. Pour mettre fin à l'annonce, appuyez à nouveau sur la touche fonction, ou appuyez sur la touche du haut-parleur. Une fois l'annonce terminée, la diode lumineuse s'éteint à nouveau.

Si un téléphone système est destinataire d'une annonce, le numéro d'appel de l'annonceur apparaît à l'écran du téléphone. L'annonce est précédée d'une tonalité de signalement diffusée par le haut-parleur. Pour mettre fin à l'annonce, appuyer sur la touche ESC.

Une touche fonction peut également être configurée sur un téléphone système pour bloquer ou autoriser les annonces.

Annonce individuelle

Par la numérotation du numéro d'appel interne d'un téléphone, vous pouvez lancer l'annonce de manière ciblée. L'annonce peut être autorisée ou bloquée par l'abonné destinataire à l'aide d'une procédure opérationnelle. Chez l'abonné destinataire ainsi que l'annonceur, l'annonce est précédée d'une tonalité de signalement.

Annonce équipe

Par la numérotation d'un numéro d'appel d'équipe, une annonce peut également être faite à une équipe. Les abonnés équipe entendent l'annonce simultanément. Chez les abonnés destinataires ainsi que l'annonceur, l'annonce est précédée d'une tonalité de signalement. L'annonce à une équipe peut également être déclenchée par une mise en attente. Avec une annonce d'équipe, il peut survenir un délai de jusqu'à quatre secondes avant que la connexion aux abonnés individuels de l'équipe ne soit établie. L'annonce passe ensuite pour les abonnés de l'équipe ayant accepté l'annonce durant ce délai.

Note

Les annonces sont automatiquement acceptées par les téléphones appelés par activation de la fonction mains libres, si :

- le téléphone est en veille,
- l'annonce est configurée et
- la fonctionnalité « silence du téléphone » n'est pas activée.

MWI (Message Waiting Indication)

Vous avez des messages dans votre boîte à lettre ou des emails vous attendent sur Inter-

net. Vous vérifiez constamment, mais ne savez jamais à l'avance si vous avez des nouveaux messages. Grâce à la fonctionnalité MWI, votre système reçoit les infos sur vos nouveaux messages du fournisseur correspondant. A présent, il ne vous faut plus aller dans votre boîte à lettre ou sur votre messagerie email que lorsque qu'il s'y trouvent effectivement de nouveaux messages. De plus, vous pouvez envoyer un MWI d'une boîte vocale reliée au système ou d'un téléphone système configuré comme téléphone de réception.

L'affichage ou le signalement de ces informations peut s'effectuer sur des terminaux (terminal analogique, RNIS ou téléphone système) qui prennent en charge ces fonctionnalités. Les informations MWI provenant de l'extérieur sont transmises par le système de manière transparente. Le téléphone **Gigaset**affiche en cas de MWI un symbole d'une enveloppe et un texte généré sur le téléphone, ainsi que le numéro de téléphone de l'appelant.

Appareils terminaux analogiques

- L'activation du MWI ne peut se produire qu'avec le combiné raccroché.
- S'il y a un message d'un système boîte vocale, un court appel a lieu. Selon l'appareil terminal, un symbole, un texte généré sur le téléphone ou le numéro de téléphone de l'appelant peuvent s'afficher. Si une information MWI est effacée, aucune signalisation n'a lieu.
- Pour le terminal, CLIP doit être configuré et autorisé dans la configuration.
- Il est possible de rappeler le système boîte vocale ou le téléphone de réception. L'information MWI est alors effacée.

Terminaux RNIS

- L'activation du MWI peut se produire à tout moment (même pendant une communication).
- S'il y a un message d'un système boîte vocale, un court appel a lieu. Selon l'appareil terminal, un symbole, un texte généré sur le téléphone ou le numéro de téléphone de l'appelant peuvent s'afficher. Si une information MWI est effacée, aucune signalisation n'a lieu.
- Il est possible de rappeler le système boîte vocale ou le téléphone de réception. L'information MWI est alors effacée.

Téléphones système

- L'activation du MWI peut se produire à tout moment (même pendant une communication). Le numéro d'appel de l'appelant est entré dans la liste des appelants. Selon le type de téléphone système, ex. boîte vocale externe, le nom ainsi que le numéro de l'appelant sont saisis. De plus, le LED **Liste des appelants** clignote.

- Il est possible de rappeler le système boîte vocale ou le téléphone de réception. L'information MWI est alors effacée.

Téléphone de chambre

- S'il y a un message d'un système boîte vocale, une tonalité de numérotation spéciale est signalée après décrochage du combiné.

Téléphone de réception

- A partir d'un téléphone de réception, à l'aide d'une procédure de téléphone, les informations MWI peuvent être activées et désactivées sur un téléphone de chambre. Si une information MWI est activée sur un téléphone de chambre, le numéro d'appel du téléphone de réception est entré dans la liste des appelants, et la tonalité de numérotation spéciale est activée.

Désactivation du message MWI

- Désactivation manuelle par procédure de téléphone à partir du téléphone de réception.
- Appel du téléphone de réception au téléphone de chambre. Dans le statut appel, les informations MWI sont automatiquement supprimées.
- Un rappel du téléphone de chambre au téléphone de réception supprime les informations MWI.

Note

Cette fonctionnalité doit être commandée à votre opérateur réseau pour votre connexion RNIS. Il vous informera des services disponibles. Les informations peuvent à présent être affichées au terminal RNIS, si un MSN externe a été attribué au terminal à la configuration.

Après un reset système, toutes les informations MWI sont supprimées.

Net Direct (clavier)

Vous aviez acheté ce qui était à l'époque le plus moderne des téléphones. Depuis sont apparus sur le Net nombre de nouvelles fonctionnalités que vous ne pouvez pas utiliser en pressant simplement une touche. A l'aide de la fonction clavier, vous pouvez, en saisissant une suite de touches, aussi utiliser les dernières fonctionnalités RNIS de votre opérateur de réseau à partir de votre téléphone RNIS ou analogique.

Par la saisie de séries de signes et de chiffres, la fonction clavier permet le pilotage de services ou de fonctionnalités dans le réseau de votre opérateur.

Note

Vous pouvez uniquement utiliser la fonctionnalité clavier si elle est prise en charge par votre opérateur de réseau, et si elle a été commandée pour votre connexion RNIS. Si vous avez configuré l'accès automatique au réseau public pour un abonné interne, les fonctions clavier ne peuvent pas être directement utilisées. Désactivez l'**Ligne extérieure automatique** préalablement ou actionnez la touche étoile, puis le code pour l'accès manuel au réseau public (ex. 0), ensuite la numérotation clavier, à commencer par la touche étoile ou dièse.

Les fonctions clavier peuvent uniquement être utilisées à partir de périphériques auxquels ont été attribué un numéro d'abonné multiple (MSN) à la configuration, et qui disposent d'une autorisation clavier.

Les fonctionnalités de votre opérateur de réseau sont toujours configurées pour le numéro d'appel envoyé par votre périphérique (MSN).

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Recevoir des communications interphone	Indiquez si les appels interphone vers le téléphone système sont permis pour cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Annonce	Indiquez si cette classe d'autorisation peut recevoir des annonces. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Recevoir les informations MWI	Indiquez si cette classe d'autorisation peut recevoir des informations sur les messages existants (MWI = Messages Waiting Indication). Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Champ	Description
Net Direct (Keypad)	Indiquez si vous voulez, par la saisie d'une suite de touches, utiliser les dernières fonctionnalités RNIS de votre opérateur de réseau, également à partir de téléphones RNIS ou analogique plus anciens. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

5.2.2.3 Applications

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Applications** des applications supplémentaires sont configurées.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Applications** se compose des champs suivants :

Champs du menu Autorisation

Champ	Description
Utilisation du répertoire téléphonique du système	Indiquez si cette classe d'autorisation peut utiliser les entrées dans le répertoire téléphonique, et, si oui, à quel degré. Valeurs possibles : • *Oui, en fonction de l'autorisation de numérotation* (valeur par défaut) : Les entrées du répertoire téléphone système peuvent être utilisées, du moment qu'elles ne se situent pas en dehors des autorisations de numérotation configurées. • *Oui, illimité* : Les entrées du répertoire téléphone système peuvent être utilisées sans restriction. • *Non* : Les entrées du répertoire téléphone système ne peuvent pas être utilisées.
Musique d'attente (MoH)	Indiquez si --et si oui, quelle-- MoH (Music on Hold) doit être utilisée. Valeurs possibles : • *Arrêt* (valeur par défaut) : Aucune musique d'attente ne doit être diffusée pour l'appelant mis en attente. • *<fichier MoH-Wave>*: L'appelant mis en attente doit en-

Champ	Description
	tendre le fichier Wave sélectionné en musique d'attente. • *MoH Intern 1* • *MoH Intern 2* • *MoH Wave 1 à 8*
Autorisation TFE	Indiquez si cette classe d'autorisation peut se connecter au portier. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
TAPI	Indiquez si cette classe d'autorisation peut utiliser les fonctionnalités TAPI. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Enregistrer les données de connexion	Indiquez si les données de connexion de cette classe d'autorisation doivent être sauvegardées. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Transmission des coûts	Indiquez si les données tarifaires transmises doivent être transmises aux terminaux de cette classe d'autorisation. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

5.2.3 Appel en parallèle

Dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Appel en parallèle** vous configurez si, avec des appels entrants sur un numéro interne, il doit y avoir une signalisation en parallèle sur un autre numéro d'appel externe.

5.2.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour créer d'autres entrées.

Le menu **Numérotation**->**Paramètres de l'utilisateur**->**Appel en parallèle**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Numéro d'appel interne	Sélectionnez le numéro d'appel interne pour lequel la fonctionnalité appel en parallèle doit être configurée.
Numéro d'appel externe	Dans **Nouveau numéro d'appel** entrez le numéro de téléphone externe auquel un appel doit être signalé en parallèle. Si un numéro de portable et un numéro d'appel personnel sont créés dans **Utilisateur**->**Configuration de base**->**Numéros d'appels externes**, ceux-ci sont indiqués dans **Numéro d'appel privé configuré** ou **Configuration du numéro de mobile** et peuvent être sélectionnés.
Appel en parallèle	Indiquez si cette entrée appel parallèle doit être activée. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

5.3 Groupes et équipes

Ce menu permet de configurer les équipes de votre système.

5.3.1 Teams

Le menu **Numérotation**->**Groupes et équipes**->**Teams** permet de configurer les équipes de votre système.

Les équipes sont des groupes de personnes qui travaillent ensemble à la réalisation d'un objectif. En pratique, cela signifie que toutes les personnes d'une équipe sont joignables via un numéro d'appel commun pour les appels externes et internes. Dans le système de télécommunications, il est ainsi possible d'affecter un numéro d'appel de façon ciblée à chaque équipe de téléphones / d'appareils terminaux, de manière à garantir l'accessibilité en cas d'appels internes et externes. Les structures individuelles des entreprises peuvent être représentées en fonction des équipes. Les différents services (vente, après-vente, développement) peuvent ainsi être appelés de manière ciblée via des numéros d'appel d'équipe en interne ou depuis l'extérieur. Au sein d'une équipe, l'appel peut par exemple être signalé en même temps à tous les téléphones, ou d'abord à un téléphone, puis à un

deuxième, etc. Des répondeurs ou des systèmes boîte vocale peuvent également être utilisés dans une équipe.

Quatre variantes d'appel sont affectées à chaque équipe. La commutation de la variante d'appel peut s'effectuer manuellement ou via l'un des calendriers.

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer une nouvelle équipe.

5.3.1.1 Général

Le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Général** permet de configurer les conditions de base de l'équipe, notamment, le nom de l'équipe et le numéro d'appel interne.

Pour les appels d'équipe internes, un numéro d'appel et un nom peuvent être attribués à l'équipe dans la configuration. Si un numéro d'appel d'équipe est sélectionné, l'appelant voit le nom de l'équipe s'afficher, jusqu'à ce qu'un abonné de l'équipe réponde. Ensuite, le nom de l'abonné de l'équipe s'affiche.

Le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une désignation pour l'équipe.
Numéro d'appel interne	Saisissez le numéro d'appel interne de l'équipe.

Champs du menu Autres paramètres

Champ	Description
Commuter la variante d'appel	Indiquez si la variante d'appel définie pour l'équipe doit être activée manuellement via le téléphone ou via le calendrier. Pour ce faire, le calendrier et les heures de commutation doivent être configurés auparavant. Pour chaque équipe, vous pouvez définir jusqu'à quatre variantes d'appel dans le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Nouveau**->**Variante 1-4**. Valeurs possibles :

Champ	Description
	• *Pas de calendrier, uniquement manuel* : la commutation manuelle est activée. • *<Calendrier>* : sélectionnez l'un des calendriers configurés.
Variante active (jour)	Sélectionnez la variante d'appel qui doit actuellement être activée. Si une commutation est définie via le calendrier, ce paramètre est à nouveau modifié en temps utile.
Autoriser le transfert des appels	Indiquez si un transfert des appels doit être effectué pour l'équipe. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Transfert des appels vers des numéros externes	Indiquez si un transfert des appels doit avoir lieu dans le système en lui-même (**Via le système**) ou via un central (fournisseur, **Via le central**). Notez qu'en cas de transfert d'appels dans le système, deux connexions externes sont occupées.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Horloge

Champ	Description
Temps de franchissement	Saisissez ici le **Temps de franchissement** après lequel un transfert d'appel doit être effectué vers l'équipe. La valeur par défaut est *15* secondes.
Appel en parallèle après le temps	En cas d'appel d'équipe (linéaire ou en rotation), il est possible d'appeler en même temps tous les abonnés de l'équipe après un délai défini. La valeur par défaut est *60* secondes.
Post-traitement	Cette configuration n'est activée que pour **Signalisation** *Uniforme*. Chaque abonné qui met fin à une communication dispose d'une durée de **post-traitement** définie pour chaque équipe et pendant laquelle il ne reçoit plus d'autre appel. Les appels que

Champ	Description
	l'abonné ne reçoit pas via l'équipe mais directement sur son numéro d'appel, ainsi que les communications qu'il initie lui-même, ne sont pas comptabilisés dans ce délai. La valeur par défaut est *0* seconde, la plage de valeurs s'étend de *0* à *999* secondes.

5.3.1.2 Variante 1 - 4

Le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Variante 1-4** permet de configurer les quatre variantes d'appel d'une équipe. Vous pouvez définir jusqu'à quatre variantes d'appel différentes pour chaque équipe. Pour ce faire, vous pouvez affecter aux variantes d'appel des numéros d'appel internes ou un numéro d'appel externe, et définir la manière dont un appel entrant doit être signalé au sein de l'équipe.

Numéros d'appel internes d'une équipe

Sous **Affectation interne**, sélectionnez les abonnés internes qui doivent appartenir à cette équipe. Si vous souhaitez exclure momentanément un abonné de la signalisation des appels (p. ex. s'il est en congé), vous pouvez sélectionner l'option **Déconnexion**. Les appels d'équipe ne sont pas signalés auprès des abonnés déconnectés. Chaque abonné de l'équipe peut également procéder lui-même à l'activation ou à la désactivation à l'aide d'un code du système.

Pour les appels d'équipe internes, un numéro d'appel et un nom peuvent être attribués à l'équipe dans la configuration. Si un numéro d'appel d'équipe est sélectionné, l'appelant voit le nom de l'équipe s'afficher, jusqu'à ce qu'un abonné de l'équipe réponde. Ensuite, le nom de l'abonné de l'équipe s'affiche. L'appel à une équipe peut se produire en rotation, de manière linéaire, simultanée, cumulative ou parallèle selon l'heure. En cas d'appel d'équipe (linéaire ou en rotation), il est possible d'appeler en même temps tous les abonnés de l'équipe après un délai défini (compris entre 1 et 99 secondes).

Le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Variante** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Affectation	Vous pouvez affecter plusieurs numéros d'appel internes ou un numéro d'appel externe à chaque équipe. Indiquez si les appels destinés à une équipe doivent être signalés aux abonnés internes ou externes. Valeurs possibles :

Champ	Description
	• *Externe* : le numéro d'appel externe entré est appelé. • *Interne* (valeur par défaut) : les abonnés affectés aux numéros d'appel sélectionnés sont appelés selon la signalisation configurée.
Affectation interne	Uniquement si **Affectation** = *Interne* Sélectionnez les abonnés internes de l'équipe. Ajoutez des numéros d'appel internes à l'aide de l'option **Ajouter**.
Affectation externe	Uniquement si **Affectation** = *Externe* Saisissez le numéro d'appel de l'abonné externe.
Affectation pour rejet et tarifs	Uniquement si **Affectation** = *Externe* L'abonné interne sélectionné détermine les frais liés à l'appel et à l'établissement d'une communication externe.

Prise d'appel automatique au sein de l'équipe

Vous souhaitez que l'appel d'un appelant soit accepté pendant la signalisation de l'appel et qu'il n'entende pas le signal d'appel (la tonalité). C'est possible si vous utilisez la prise d'appel automatique pour les appels d'équipe. Dans ce cas, l'appel est accepté automatiquement par le système, et l'appelant entend une annonce ou une musique d'attente. Pendant ce temps, l'appel est signalé aux abonnés définis de l'équipe. Si un abonné accepte l'appel, la communication avec l'appelant est établie.

En cas d'appel à une équipe, il est possible, dans la configuration, de définir la prise automatique de l'appel. L'appelant entend alors une annonce ou une musique. Pendant de ce temps, le ou les abonnés de destination sont appelés. Une fois le combiné décroché, l'annonce ou la musique est arrêtée, et la communication est établie.

Paramètres possibles pour la prise d'appel automatique :

- *Simultané* : tous les appareils terminaux attribués sont appelés simultanément. Si un appareil terminal est occupé, il est possible d'émettre un signal d'appel en attente.
- *Linéaire* : tous les appareils terminaux attribués sont appelés de manière successive dans l'ordre indiqué dans la configuration. Si un appareil terminal est occupé, l'appareil terminal libre suivant est appelé. L'appel est signalé pendant env. 15 secondes à chaque abonné. Cette durée peut être réglée entre 1 et 99 secondes (pour chaque équipe). Si des abonnés téléphonent ou s'ils sont déconnectés, il n'y a aucun délai de

transmission pour ces abonnés.

- *En rotation* : cet appel est une exception à l'appel linéaire. Une fois que tous les appareils terminaux ont été appelés, la signalisation de l'appel recommence à partir du premier appareil terminal entré. L'appel est signalé jusqu'à ce que l'appelant raccroche ou jusqu'à ce que le central y mette fin (après env. deux minutes).
- *Création* : les appareils terminaux sont appelés dans l'ordre indiqué dans la liste des abonnés. Chaque appareil terminal déjà appelé est rappelé, jusqu'à ce que tous les appareils terminaux entrés aient été appelés.
- *Linéaire, parallèle selon l'heure* : une configuration linéaire ou en rotation peut être définie pour les appels d'équipe. Une fois la durée définie écoulée, tous les abonnés de l'équipe peuvent être appelés en parallèle (simultanément). Exemple : Condition préalable : la somme des temps de franchissement doit être supérieure à la durée **parallèle selon l'heure**. Quatre abonnés se trouvent dans une équipe. Le temps de franchissement s'élève à 10 secondes pour chaque abonné (40 secondes au total). La durée **parallèle selon l'heure** est définie sur 38 secondes. Chacun des abonnés est appelé. Si un abonné se déconnecte ou s'il est occupé, le temps de franchissement ne s'élève plus qu'à 30 secondes. Ensuite, l'appel **parallèle selon l'heure** n'est plus effectué.
- *Uniforme* : la répartition uniforme correspond à la configuration suivante : **Signalisation En rotation**. Elle fait en sorte que tous les abonnés d'une équipe reçoivent le même nombre d'appels. Chaque abonné qui met fin à une communication dispose d'une durée de **Post-traitement** (comprise entre 0 et 999 secondes) définie pour chaque équipe / abonné et pendant laquelle il ne reçoit plus d'autre appel. Les appels que l'abonné ne reçoit pas via l'équipe mais directement sur son numéro d'appel, ainsi que les communications qu'il initie lui-même, ne sont pas comptabilisés dans la répartition uniforme. La répartition uniforme commence avec l'abonné qui n'a plus reçu d'appel depuis le plus longtemps, ou, après un redémarrage, avec le premier abonné entré dans la liste. Un abonné qui s'est déconnecté (code ou touche de fonction) est ignoré dans le cadre de la répartition uniforme. Après une panne de courant sur le système, le calcul existant relatif à la **répartition uniforme** est supprimé et le processus recommence. Si tous les abonnés de l'équipe sont en **post-traitement**, les appels externes sont renvoyés vers la destination de rejet définie ; les appelants internes entendent la sonnerie « occupé ». Si, pour plusieurs abonnés de l'équipe, la même durée est calculée après la fin de leur dernier appel, c'est l'ordre des entrées de l'**Affectation interne** qui prévaut.

Champs du menu Options

Champ	Description
Signalisation	Vous pouvez appeler les abonnés d'une équipe en utilisant l'appel général. Valeurs possibles :

Champ	Description
	• *Simultané* (valeur par défaut) • *Linéaire* • *En rotation* • *Création* • *Linéaire, parallèle selon l'heure* • *En rotation, parallèle selon l'heure* • *Uniforme*
Occupé par occupé (Busy on Busy)	Indiquez si, pour cette variante d'appel, la fonctionnalité « Busy on Busy » doit être activée. Si un abonné d'une équipe est en communication, vous pouvez indiquer si d'autres appels destinés à cette équipe doivent être signalés. Si la fonction « Busy on Busy » est activée pour cette équipe, les autres appelants entendent le signal « occupé ». Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Prise d'appel automatique avec	Indiquez si un appel entrant doit être accepté automatiquement et si l'appelant doit entendre l'annonce ou la musique d'attente sélectionnée. L'appel est ensuite signalé à l'équipe. Les frais liés à la communication existante sont pris en charge par l'appelant. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Sélectionnez également l'annonce ou la musique d'attente de votre choix. Valeurs possibles : • *<Fichier_x>* • *MoH Intern 1* • *MoH Intern 2* • *MoH Wave 1 à 8*

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Fonctions de rejet

Champ	Description
Rejet en absence de réponse	Indiquez si un appel entrant doit être renvoyé en cas d'absence de réponse et, si tel est le cas, vers quelle équipe. Valeurs possibles : • *aucun* • *<Equipe>* Saisissez également le délai après lequel le rejet doit être effectué.
Autres fonctions de rejet	Indiquez si un appel entrant doit être transféré et, si tel est le cas, via quelle variante de rejet. Valeurs possibles : • *Arrêt* : aucune autre variante de rejet n'est utilisée. • *Immédiatement* : l'appel entrant est directement transféré via la fonction de rejet sélectionnée dans **Immédiatement**. • *Si occupé* : l'appel entrant est transféré via la fonction de rejet sélectionnée dans **Si occupé**.
Immédiatement	Uniquement si **Autres fonctions de rejet** = *Immédiatement* Sélectionnez la fonction de rejet pour le rejet immédiat. Vous pouvez configurer les fonctions de rejet sous **Applications**->**Rejet**->**Fonctions de rejet**.
Si occupé	Uniquement si **Autres fonctions de rejet** = *Si occupé* Sélectionnez la fonction de rejet pour le rejet en cas de ligne occupée. Vous pouvez configurer les fonctions de rejet sous **Applications**->**Rejet**->**Fonctions de rejet**.
Occupé en commençant par	Uniquement si **Autres fonctions de rejet** = *Si occupé* Indiquez le nombre d'abonnés à partir duquel l'équipe doit être considérée comme occupée.

5.3.1.3 Ouverture/fermeture de session

Le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Ouverture/fermeture de session** permet de connecter ou de déconnecter les membres de l'équipe individuellement.

Le menu **Numérotation**->**Groupes et équipes**->**Teams**->**Ouverture/fermeture de session** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Numéros d'appel	Permet d'afficher le numéro d'appel interne des membres de l'équipe affectés.
État	Indiquez si le membre de l'équipe est connecté à l'équipe. Sélectionnez *Connecté* pour connecter le membre de l'équipe.

5.4 Répartition des appels

Ce menu permet de configurer le transfert interne de tous les appels entrants.

5.4.1 Affectation des appels

Le menu **Numérotation**->**Répartition des appels**->**Affectation des appels** permet de configurer l'attribution des appels entrants aux numéros d'appel internes souhaités.

L'affectation des appels permet d'attribuer les numéros d'appel entrés sous **Numéros d'appels externes** aux équipes ou à un numéro d'appel interne, par exemple.

5.4.1.1 Editer

Sélectionnez le symbole pour traiter les entrées existantes.

Le menu **Numérotation**->**Répartition des appels**->**Affectation des appels**-> se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
<Nom du numéro d'appel entré>	Permet d'afficher le numéro d'appel configuré.
Connexion externe	Permet d'afficher la connexion externe pour laquelle l'affectation des appels a été configurée.
Affectation	Sélectionnez la fonction ou le numéro d'appel interne auquel vous souhaitez attribuer les appels entrants via la ligne sélectionnée dans **Connexion externe**. Valeurs possibles : • *Numéro interne* (valeur par défaut) : Le numéro d'appel interne de l'équipe est sélectionné pour l'attribution à une équipe. • *Call Through* • *Application de rejet* • *Accès distant Téléphonie* • *Identifiant RNIS* • *Identifiant service* • *Centre d'appel mini*

Champs du menu Paramètres numéro d'appel interne et rejet

Champ	Description
Numéro d'appel interne	Uniquement pour **Affectation** = *Numéro d'appel interne* Sélectionnez le numéro d'appel interne auquel vous souhaitez attribuer les appels entrants via la ligne sélectionnée dans **Connexion externe**.
Application du rejet	Uniquement pour **Affectation** = *Application de rejet* Sélectionnez l'application de rejet que vous souhaitez attribuer au numéro d'appel. Le menu **Applications**->**Rejet**->**Applications du rejet** permet de configurer les applications de rejet.
Variante active (jour)	Uniquement pour Application de rejet = *<Application de rejet configurée>* Sélectionnez la variante de l'application de rejet (qui doit ac-

Champ	Description
	tuellement être activée). Si une commutation des variantes est définie via le calendrier, ce paramètre est à nouveau modifié en temps utile. Valeurs possibles : • *Variante 1* • *Variante 2* • *Variante 3* • *Variante 4*

Champs du menu Paramètres Call Through

Champ	Description
Autorisation d'accès	Uniquement pour **Affectation** = *Call Through* Déterminez l'autorisation en vertu de laquelle la fonction Call Through est activée. Valeurs possibles : • *Vérification du numéro d 'appel* : l'activation de la numérotation s'effectue après la vérification du numéro d'appel entré avec l'entrée du répertoire téléphonique du système ou avec les numéros d'appel entrés de l'utilisateur (**Numéro de mobile** et **Numéro d'appel privé**). • *Numéros d'appel et PIN* : l'activation de la numérotation s'effectue après la vérification du numéro d'appel entré avec l'entrée du répertoire téléphonique du système ou avec les numéros d'appel entrés de l'utilisateur (**Numéro de mobile** et **Numéro d'appel privé**) ET la saisie du PIN. • *PIN* : l'activation de la numérotation s'effectue après la saisie du PIN. • *Numéro d'appel ou PIN* : l'activation de la numérotation s'effectue après la vérification du numéro d'appel entré avec l'entrée du répertoire téléphonique du système ou avec les numéros d'appel entrés de l'utilisateur (**Numéro de mobile** et **Numéro d'appel privé**) OU la saisie du PIN.
PIN (6 caractères)	Uniquement pour **Autorisation d'accès** = *Numéros d'appel et PIN*, *PIN*, *Numéro d'appel ou PIN*

Champ	Description
	Le système vérifie l'autorisation de l'appelant pour le transfert de l'appel et simule l'activation d'une tonalité de numérotation externe. L'autorisation est accordée si l'appelant a saisi le bon PIN à six chiffres.
Paramètres numéro d'appel interne et rejet	Sélectionnez l'abonné interne via lequel l'appel Call Through doit être effectué. Un des numéros de téléphone du système est défini pour la fonction Call Through dans la configuration. Une sonnerie de signalement du système retentit d'abord pour l'appelant externe qui établit une communication sur ce numéro de téléphone.

5.4.2 Rejet si numérotation erronée

Le menu **Numérotation**->**Répartition des appels**->**Rejet si numérotation erronée** permet de définir, pour chaque connexion externe, l'équipe ou l'abonné vers lequel l'appel doit être effectué si

- le numéro d'appel / la numérotation directe est incomplète ou erronée pour un appel entrant ;
- tous les abonnés de l'équipe ou du centre d'appel sélectionné sont déconnectés ;
- tous les abonnés du centre d'appel sélectionné sont en post-traitement.

5.4.2.1 Editer

Sélectionnez le symbole pour traiter les entrées existantes.

Le menu **Numérotation**->**Répartition des appels**->**Rejet si numérotation erronée**-> se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Connexion externe	Permet d'afficher la connexion externe pour laquelle l'option Rejet si numérotation erronée est configurée.
Rejet vers un numéro d'appel	Sélectionnez le type de rejet. Valeurs possibles : • *aucun* : aucun rejet n'est effectué ; l'appelant reçoit le signal

Champ	Description
	« occupé ». • *Paramètres globaux* : le rejet s'effectue comme défini sous **Gestion du système**->**Paramètres globaux**->**Système**->**Rejet vers un numéro d'appel**. • *<Numéro d'appel interne d'un utilisateur ou d'une équipe>* : Le rejet est effectué via cet utilisateur ou cette équipe.

Chapitre 6 Appareil terminal

6.1 Gigaset Téléphone

Ce menu permet d'attribuer les numéros d'appel internes configurés aux appareils terminaux et de définir d'autres fonctions, selon le type d'appareil.

Les appareils terminaux des téléphones système sont triés par ordre alphabétique dans la colonne **Description**. Vous pouvez cliquer sur le titre de toute autre colonne et trier les entrées dans l'ordre croissant ou décroissant.

6.1.1 Gigaset Téléphone

Le menu **Appareil terminal**->**Gigaset Téléphone**->**Gigaset Téléphone** permet d'affecter les numéros d'appel internes configurés aux téléphones IP raccordés.

Les téléphones IP raccordés sont identifiés automatiquement et répertoriés dans la section inférieure de l'aperçu.

Sélectionnez le symbole pour traiter les entrées existantes. Dès qu'une **Description** est entrée pour un téléphone et validée avec **OK**, l'entrée pour cet appareil est placée dans la section supérieure de l'aperçu.

Pour la suite de la configuration, cliquez de nouveau sur le symbole .

Sélectionnez le bouton **Nouveau** pour configurer manuellement un autre appareil terminal IP.

Sélectionnez le bouton pour accéder à la page administrateur de l'interface utilisateur du téléphone **Gigaset**. Une description est disponible dans le mode d'emploi du téléphone.

6.1.1.1 Général

Le menu **Appareil terminal**->**Gigaset Téléphone**->**Gigaset Téléphone**->**Général** permet de procéder au paramétrage de base d'un téléphone IP.

Le menu **Appareil terminal**->**Gigaset Téléphone**->**Gigaset Téléphone**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Afin de pouvoir identifier clairement le téléphone dans le système, saisissez-en une description.
Type de téléphone	Permet d'afficher le type de votre téléphone IP. Valeurs possibles : • *DE310 IP PRO* • *DE410 IP PRO* • *DE700 IP PRO* • *DE900 IP PRO*
Emplacement	Sélectionnez l'emplacement du téléphone. Le menu **VoIP**->**Paramètres**->**Emplacements** permet de définir les emplacements. Selon les paramètres de ce menu, vous pouvez sélectionner le comportement par défaut pour l'enregistrement de participants VoIP, pour lesquels aucun emplacement ne doit être défini. Valeurs possibles : • *Non défini (enregistrement incorrect)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné est néanmoins enregistré. • *Non défini (pas d'enregistrement)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné n'est pas enregistré. • *Non défini (enregistrement seulement dans des réseaux privés)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné n'est enregistré que s'il se trouve dans un réseau privé. • *<Emplacement>* : Un emplacement défini est sélectionné. L'abonné n'est enregistré que s'il se trouve à cet emplacement.
Adresse MAC	Permet d'afficher l'adresse MAC du téléphone.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Autres paramètres

Champ	Description
Pas d'attente et récupération	Les fonctionnalités de mise en attente et de récupération d'un appel ne sont pas disponibles sur certains téléphones. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Champs du menu Paramètres Codex

Champ	Description
Profil Codec	Sélectionnez le profil Codec à utiliser. Vous pouvez configurer le profil Codec dans le menu **VoIP**->**Paramètres**->**Profils Codec**

6.1.1.2 Numéros d'appel

Le menu **Appareil terminal**->**Gigaset Téléphone**->**Gigaset Téléphone**->**Numéros d'appel** permet d'affecter à un téléphone IP jusqu'à douze numéros d'appel internes avec **Ajouter**.

Les numéros d'appel internes disponibles sont créés sous **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Nouveau**.

permet d'effacer de la liste les numéros d'appel affectés.

Valeurs de la liste Paramètres du numéro d'appel

Champ	Description
N° de connexion	Indique le numéro d'ordre de la connexion.
Numéro d'appel interne	Permet d'afficher le numéro d'appel interne affecté.
Description affichée	Affiche la description qui apparaît sur l'écran du téléphone IP.
Utilisateur	Permet d'afficher le nom de l'utilisateur.

6.1.1.3 Paramètres

Le menu **Appareil terminal**->**Gigaset Téléphone**->**Gigaset Téléphone**->**Paramètres** permet de réinitialiser le mot de passe administrateur du téléphone.

Le menu **Appareil terminal**->**Gigaset Téléphone**->**Gigaset Téléphone**->**Paramètres** se compose des champs suivants :

Champs du menu Gigaset Téléphone

Champ	Description
Mot de passe administrateur	Indiquez si le mot de passe administrateur doit être réinitialisé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Dès que vous sélectionnez le bouton **OK**, le mot de passe est réinitialisé en fonction des paramètres de base.

6.1.2 Gigaset DECT

Le menu **Appareil terminal**->**Gigaset Téléphone**+**Gigaset DECT** affiche les stations de base des systèmes SingleCell et MultiCell DECT connectés.

Les stations de base raccordées sont identifiées automatiquement et répertoriées dans la section inférieure de l'aperçu. (DHCP est requis pour cela.)

Sélectionnez le symbole pour traiter les entrées existantes. Dès qu'une **Description** est entrée pour uns station de base et validée avec **OK**, l'entrée pour cet appareil est placée dans la section supérieure de l'aperçu. Après une courte durée, les symboles et pour cet appareil sont affichés.

Pour pouvoir utiliser le provisionnement automatique, cliquez de nouveau sur le symbole et ajoutez le numéro d'appel correspondant.

Sélectionnez le bouton **Nouveau** pour configurer manuellement une autre station de base.

Sélectionnez le bouton pour accéder au programme de configuration basé sur le Web de la station de base. Il est décrit dans le mode d'emploi du système DECT

Utilisez le provisionnement automatique pour utiliser **elmeg hybird** afin de transférer des paramètres de téléphonie élémentaires au système DECT. Si vous voulez pour cela utiliser l'assistant **Premiers pas**, activez sous **Assistant**->**Premiers pas**->**Paramètres avancés**->**Ajouter** dans le champ **Transférer le serveur de provisionnement pour** la valeur *Gigaset DECT*. Vous pouvez autrement définir sous **Services locaux**->**Serveur DHCP**->**Configuration DHCP**->**Nouveau**->**Paramètres avancés** les champs **Option** = *URL (Serveur de provisionnement)* et **Valeur** = *http://<IP_Adresse des Provi-*

sionierungsservers>/eg_prov.

Pour connecter les unités mobiles, placez tout d'abord la station de base en mode de connexion. Procédez ensuite à la connexion des unités mobiles aux unités mobiles elles-mêmes. Vous devez réaliser une configuration plus complète de la station de base à l'aide du programme de configuration basé sur le Web du système DECT.

Sélectionnez le bouton pour procéder à la mise à jour du provisionnement de l'appareil. Après une mise à jour réussie, la valeur actualisée apparaît dans la colonne **Vu en dernier** dans un délai de 10 secondes.

Note

Pour tester si votre station de base est bien configurée et accessible, sélectionnez le bouton et contrôlez si une valeur actualisée apparaît dans la colonne **Vu en dernier** dans un délai de 10 secondes.

Note

Si vous voulez modifier la langue utilisée pour un système SingleCell DECT, le système doit être connecté au serveur de provisionnement de **elmeg hybird**. Vous devez avoir une carte SD installée. Toutes les langues utilisées doivent être enregistrées sur la carte SD. Les systèmes SingleCell chargent la langue souhaitée depuis la carte SD si nécessaire.

6.1.2.1 Général

Le menu **Appareil terminal**->**Gigaset Téléphone**+**Gigaset DECT**->**Général** permet de procéder au paramétrage de base des stations de base.

Le menu **Appareil terminal**->**Gigaset Téléphone**+**Gigaset DECT**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Afin de pouvoir identifier clairement la station de base dans le système, saisissez-en une description.
Type de téléphone	Permet d'afficher le type de station de base.

Champ	Description
	Valeurs possibles : • *N510 IP PRO* • *N720 DM PRO*
Emplacement	Sélectionnez l'emplacement de la station de base. Le menu **VoIP**->**Paramètres**->**Emplacements** permet de définir les emplacements. Selon les paramètres de ce menu, vous pouvez sélectionner le comportement par défaut pour l'enregistrement de participants VoIP, pour lesquels aucun emplacement ne doit être défini. Valeurs possibles : • *Non défini (enregistrement incorrect)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné est néanmoins enregistré. • *Non défini (pas d'enregistrement)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné n'est pas enregistré. • *Non défini (enregistrement seulement dans des réseaux privés)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné n'est enregistré que s'il se trouve dans un réseau privé. • *<Emplacement>* : Un emplacement défini est sélectionné. L'abonné n'est enregistré que s'il se trouve à cet emplacement.
Adresse MAC	Permet d'afficher l'adresse MAC de la station de base.
Liaison IP/MAC	Permet d'afficher l'adresse IP attribuée automatiquement par DHCP. Vous pouvez ici affecter de manière fixe l'adresse IP affichée à la station de base avec l'adresse MAC affichée. Pour permettre un rappel rapide après un dysfonctionnement, cette option doit être activée.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Autres paramètres

Champ	Description
Pas d'attente et récupération	Les fonctionnalités de mise en attente et de récupération d'un appel ne sont pas disponibles sur certains téléphones. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Champs du menu Paramètres Codex

Champ	Description
Profil Codec	Sélectionnez le profil Codec à utiliser. Vous pouvez configurer le profil Codec dans le menu **VoIP**->**Paramètres**->**Profils Codec**.

6.1.2.2 Numéros d'appel

Le menu **Appareil terminal**->**Gigaset Téléphone**+**Gigaset DECT**->**Numéros d'appel** permet d'affecter les unités mobiles **Numéros d'appel internes**. Vous pouvez sélectionner d'après les numéros d'appel créés pour cela sous **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**.

Un numéro d'ordre, **Numéro de mobile**, est automatiquement affecté par le système à chaque unité mobile. Il permet d'identifier l'appareil. Vous pouvez ensuite utiliser **Ajouter** pour affecter à une unité mobile exactement un **Numéro d'appel interne** de la liste.

permet d'effacer les numéros d'appel affectés.

Valeurs de la liste Numéros d'appel

Champ	Description
Numéro de mobile	Indique le numéro d'ordre de l'unité mobile. Ce numéro est affecté à l'unité mobile afin de pouvoir l'identifier clairement.
Numéro d'appel interne	Permet d'afficher le numéro d'appel interne affecté.
Description affichée	Permet d'afficher la description saisie pour le numéro d'appel interne. Cette description est affichée en mode de repos sur l'écran de l'unité mobile.
Utilisateur	Permet d'afficher le nom de l'utilisateur.

6.1.2.3 Paramètres

Le menu **Appareil terminal**->**Gigaset Téléphone**+**Gigaset DECT**->**Paramètres** permet de réinitialiser le mot de passe administrateur de la station de base.

Le menu **Appareil terminal**->**Gigaset Téléphone**+**Gigaset DECT**->**Paramètres** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Mot de passe administrateur	Indiquez si le mot de passe administrateur doit être réinitialisé. Sélectionnez `Activé` pour activer la fonction. La fonction est désactivée par défaut. Dès que vous sélectionnez le bouton **OK**, le mot de passe est réinitialisé en fonction des paramètres de base.

6.2 Autres téléphones

Ce menu permet d'attribuer les numéros d'appel internes configurés aux appareils terminaux et de définir d'autres fonctions, selon le type d'appareil.

Les appareils terminaux des différentes catégories (VoIP, ISDN ou analogique) des téléphones système sont triés par ordre alphabétique dans la colonne **Description**. Vous pouvez cliquer sur le titre de toute autre colonne et trier les entrées dans l'ordre croissant ou décroissant.

6.2.1 VoIP

Le menu **Appareil terminal**->**Autres téléphones**->**VoIP** permet de configurer les appareils terminaux VoIP connectés. Vous procédez par exemple à l'affectation d'un numéro d'appel interne configuré.

6.2.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des appareils terminaux VoIP.

Le menu **Appareil terminal**->**Autres téléphones**->**VoIP**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le téléphone IP.
Emplacement	Sélectionnez l'emplacement du téléphone. Le menu **VoIP**->**Paramètres**->**Emplacements** permet de définir les emplacements. Selon les paramètres de ce menu, vous pouvez sélectionner le comportement par défaut pour l'enregistrement de participants VoIP, pour lesquels aucun emplacement ne doit être défini. Valeurs possibles : • *Non défini (enregistrement incorrect)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné est néanmoins enregistré. • *Non défini (pas d'enregistrement)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné n'est pas enregistré. • *Non défini (enregistrement seulement dans des réseaux privés)* : aucun emplacement n'est défini. Selon le comportement par défaut défini, l'abonné n'est enregistré que s'il se trouve dans un réseau privé. • *<Emplacement>* : Un emplacement défini est sélectionné. L'abonné n'est enregistré que s'il se trouve à cet emplacement.

Champs du menu Paramètres du numéro d'appel

Champ	Description
Numéros d'appel internes	Sélectionnez les numéros d'appel internes pour cet appareil terminal. Vous pouvez définir plusieurs numéros d'appel internes. Valeurs possibles : • *Toutes les lignes sont occupées* : tous les numéros d'appel internes configurés sont déjà utilisés. Configurez d'abord un nouvel utilisateur avec des numéros d'appel internes.

Champ	Description
	• *<Numéro d'appel interne>* : Sélectionnez l'un des numéros d'appel existants de l'utilisateur configuré.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres client SIP

Champ	Description
Mode client SIP	Définissez si un client SIP *dynamique* ou *statique* doit être utilisé. Valeurs possibles : • *Dynamique* (valeur par défaut) : Votre appareil (par exemple un téléphone SIP standard) réalise un enregistrement SIP pour communiquer au système son adresse IP (dynamique). • *Statique* : un appel entrant d'un client SIP (configuré comme statique) est accepté par le système sans que ce client doive d'abord s'enregistrer, si l'adresse IP du client correspond à l'adresse IP entrée sous **Adresse IP du client SIP**. Ce mode est par exemple utilisé par le serveur MIcrosoft Office Communications et d'autres serveurs de communication unifiée.
Adresse IP du client SIP	Uniquement pour **Mode client SIP** = *Statique* : Saisissez l'adresse IP locale statique du client SIP.
Numéro de port	Uniquement pour **Mode client SIP** = *Statique* : Indiquez le numéro du port à utiliser pour la connexion. Il est possible d'utiliser une suite de 5 chiffres. Pour la connexion à un serveur Microsoft Exchange Communication, entrez par exemple le port *5065*.
Protocole transparent	Uniquement pour **Mode client SIP** = *Statique* : Sélectionnez le protocole transparent pour cette communication. Valeurs possibles : • *UDP* (valeur par défaut)

Champ	Description
	• *TCP* Pour la connexion à un serveur Microsoft Exchange Communication, entrez par exemple le protocole *TCP*.

Champs du menu Paramètres Codex

Champ	Description
Profil Codec	Sélectionnez le profil Codec qui doit être utilisé en cas de connexion via une ligne VoIP. Vous pouvez configurer le profil Codec dans le menu **VoIP**->**Paramètres**->**Profils Codec**.

Champs du menu Autres paramètres

Champ	Description
Autoriser les connexions multiples	Indiquez si des connexions multiples peuvent être autorisées par cet appareil terminal. Utilisation comme installation secondaire : uniquement en cas de connexion d'une installation secondaire à un système. Lorsque la fonctionnalité est désactivée, une seule connexion est possible via l'enregistrement SIP du participant. En cas d'arrivée d'un deuxième appel, il est accepté et la conversation en cours est interrompue. Lorsque la fonctionnalité est activée, plusieurs connexions SIP sont possibles avec le même enregistrement. Lorsque la fonctionnalité est désactivée pour un système sans installation secondaire, plusieurs (par exemple deux) conversations en cours simultanément sur le téléphone ne sont pas réunies mais terminées après avoir raccroché. Cette fonctionnalité ne devrait pas être activée ici. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Pas d'attente et récupération	Les fonctionnalités de mise en attente et de récupération d'un appel ne sont pas disponibles sur certains téléphones. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

6.2.2 RNIS

Le menu **Appareil terminal**->**Autres téléphones**->**RNIS** permet de configurer les appareils terminaux RNIS connectés. Vous procédez par exemple à l'affectation d'un numéro d'appel interne configuré.

6.2.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter un appareil terminal RNIS supplémentaire.

Le menu **Appareil terminal**->**Autres téléphones**->**RNIS**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le téléphone RNIS.
Interface	Sélectionnez l'interface à laquelle le téléphone RNIS est connecté.

Champs du menu Paramètres téléphoniques de base

Champ	Description
Type d'appareil terminal	Sélectionnez le type d'appareil terminal. Valeurs possibles : • *Téléphone* (valeur par défaut) • *Répondeur* • *Boîte vocale* • *Téléphone d'appel d'urgence*
Numéros d'appel internes	Sélectionnez les numéros d'appel internes pour cet appareil terminal. Vous pouvez définir plusieurs numéros d'appel internes. Valeurs possibles : • *Toutes les lignes sont occupées* : tous les numéros d'appel internes configurés sont déjà utilisés. Configurez d'abord un nouvel utilisateur avec des numéros d'appel in-

Champ	Description
	ternes. • *<Numéro d'appel interne>* : Sélectionnez l'un des numéros d'appel existants de l'utilisateur configuré.

6.2.3 Analogue

Le menu **Appareil terminal**->**Autres téléphones**->**Analogue** permet de configurer les appareils terminaux analogiques connectés. Vous procédez par exemple à l'affectation d'un numéro d'appel interne configuré.

6.2.3.1 Editer

Sélectionnez le symbole pour traiter les entrées existantes.

Sélectionnez le symbole pour copier les entrées existantes. La copie d'une entrée peut s'avérer utile lorsque vous souhaitez créer une entrée qui ne diffère que par quelques paramètres d'une entrée déjà existante. Dans ce cas, il vous suffit de copier l'entrée et de modifier les paramètres souhaités.

Le menu **Appareil terminal**->**Autres téléphones**->**Analogue**->**Editer** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le téléphone analogique.
Interface	Sélectionnez l'interface à laquelle le téléphone est connecté.

Champs du menu Paramètres téléphoniques de base

Champ	Description
Type d'appareil terminal	Sélectionnez le type d'appareil terminal. Valeurs possibles : • *Appareil multifonctions/télécopieur* • *Téléphone* • *Modem* • *Répondeur*

Champ	Description
	• *Téléphone d'appel d'urgence*
Numéro d'appel interne	Sélectionnez le numéro d'appel interne pour cet appareil terminal. Valeurs possibles : • *Toutes les lignes sont occupées* : le numéro d'appel interne configuré est déjà utilisé. Configurez d'abord un nouvel utilisateur avec des numéros d'appel internes. • *<Numéro d'appel interne>* : Sélectionnez l'un des numéros d'appel existants de l'utilisateur configuré.

Champs du menu Réglage du téléphone

Champ	Description
Signal appel en attente	Indiquez si le signal d'appel en attente est autorisé pour cet appareil terminal. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Protection d'appel (silence)	Indiquez si vous souhaitez utiliser la fonctionnalité de protection d'appel (silence du téléphone). Cette fonctionnalité vous permet de modifier la signalisation des appels sur votre appareil terminal. Les appareils terminaux analogiques utilisent pour ce faire les codes du système. Valeurs possibles : • *Pas de signal pour les appels internes* • *Pas de signal pour les appels externes* • *Aucun appel*

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres CLIP

Champ	Description
Afficher le numéro d'appel (CLIP)	Indiquez si le numéro d'appel du participant doit être transmis. Sélectionnez *Activé* pour activer la fonction.

Champ	Description
	La fonction est activée par défaut.
Afficher la date et l'heure	Uniquement pour **Afficher le numéro d'appel (CLIP)** *Activé* Indiquez si la date et l'heure de votre **hybird** doivent être reprises et affichées sur le téléphone. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Afficher le nom entrant (CNIP)	Uniquement pour **Afficher le numéro d'appel (CLIP)** *Activé* Indiquez si le nom de l'appelant doit être affiché. Le nom de l'appelant peut être affiché si une entrée est présente dans le répertoire téléphonique du système. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Afficher le numéro d'appel entrant (CLIP-Offhook)	Uniquement pour **Afficher le numéro d'appel (CLIP)** *Activé* Indiquez si le numéro d'appel d'un appelant doit être affiché pendant un signal d'appel en attente. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Champs du menu Autres paramètres

Champ	Description
Afficher les nouveaux messages (MWI)	Uniquement pour **Afficher le numéro d'appel (CLIP)** *Activé* Indiquez si de nouveaux messages doivent être signalés sur un système de messagerie vocale. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Transmettre les informations sur les coûts	Indiquez si le système doit utiliser les informations de taxation du réseau RNIS pour créer des impulsions de taxation pour l'appareil terminal. Vous pouvez déterminer si l'impulsion de

Champ	Description
	taxation doit s'élever à 12 ou à 16 kHz. Valeurs possibles : • *Arrêt* : Les informations de taxation du réseau RNIS ne sont pas transmises. • *12 kHz* • *16 kHz*
Tension alternative d'appel FXS	La signalisation des appels sur les appareils terminaux analogiques se fait par l'application d'une tension alternative d'appel sur les connexions analogiques contactées. La tension alternative d'appel est convertie en une tonalité par l'appareil analogique. Vous pouvez configurer dans le système la tension alternative d'appel pour les connexions analogiques avec une fréquence de *25 Hz* ou *50 Hz*. La valeur par défaut est *50* Hz.
Temps flash pour numérotation multi-fréquences	Lors de l'utilisation d'appareils terminaux analogiques avec numérotation à impulsion, vous pouvez régler le temps de flash identifié par le système comme longueur de flash maximale. Si le flash de l'appareil terminal est plus long que la durée définie, le système considère que le combiné est raccroché. Les valeurs possibles sont comprises entre *100 ms* (valeur par défaut) et *1000 ms*.

6.2.4 CAPI

Si votre appareil est compatible CAPI, configurez les terminaux CAPI connectés dans le menu **Appareil terminal**->**Autres téléphones**->**CAPI**. Vous procédez par exemple à l'affectation d'un numéro d'appel interne configuré.

6.2.4.1 Éditer ouNouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter un appareil terminal CAPI supplémentaire.

Le menu **Appareil terminal**->**Autres téléphones**->**CAPI**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le téléphone CAPI.

Champs du menu Paramètres téléphoniques de base

Champ	Description
Numéros d'appel internes	Sélectionnez les numéros d'appel internes pour cet appareil terminal à l'aide de l'option **Ajouter**. Vous pouvez définir plusieurs numéros d'appel internes. Valeurs possibles : • *Toutes les lignes sont occupées* : tous les numéros d'appel internes configurés sont déjà utilisés. Configurez d'abord un nouvel utilisateur avec des numéros d'appel internes. • *<Numéro d'appel interne>* : Sélectionnez l'un des numéros d'appel existants de l'utilisateur configuré.

6.3 Aperçu

6.3.1 Aperçu

Le menu **Appareil terminal**->**Aperçu**->**Aperçu** présente un aperçu de tous les appareils terminaux configurés.

Valeurs de la liste Aperçu

Champ	Description
Description	Permet d'afficher la description de l'appareil terminal.
Type de téléphone	Permet d'afficher le type de téléphone.
Interface/Emplacement	Indique pour les appareils terminaux RNIS, système et analogiques l'interface sur laquelle ils sont connectés au système. Sur les appareils terminaux IP, le site configuré est affiché.
Numéros d'appel internes	Permet d'afficher les numéros d'appel internes configurés.

Chapitre 7 Contrôle d'appel

Les fonctions pour les appels externes, les communications externes et les règles de sélection pour les communications externes sont définies dans le contrôle d'appel.

7.1 Services sortants

Le menu **Contrôle d'appel**->**Services sortants** permet de configurer les fonctionnalités **Appel direct**, **Transfert des appels (AWS)**, **Contrôle de numérotation** et **Numéro d'appel prioritaire**.

7.1.1 Appel direct

Le menu **Contrôle d'appel**->**Services sortants**->**Appel direct** permet de configurer les numéros d'appel qui se composent automatiquement, sans intervention de l'interlocuteur.

Vous souhaitez configurer un téléphone permettant d'établir une communication vers un numéro d'appel défini sans devoir composer le numéro d'appel en question (p. ex. un téléphone d'appel d'urgence). Vous êtes en déplacement. Pourtant, il y a quelqu'un à la maison que vous devez pouvoir joindre rapidement et facilement en cas de besoin (p. ex. les enfants ou les grands-parents). Si vous avez configuré la fonction « Appel direct » pour un ou plusieurs téléphones, il vous suffit de décrocher le combiné du téléphone en question. Une fois le délai configuré écoulé, en l'absence d'une autre saisie, le système sélectionne automatiquement le numéro d'appel direct défini.

Si vous n'effectuez pas de sélection dans le délai imparti après avoir décroché le téléphone, la numérotation automatique est effectuée.

Le temps de l'appel direct se configure sous **Gestion du système**->**Paramètres globaux**->**Horloge**->**Appel direct**.

Note

L'administrateur peut configurer jusqu'à 10 destinations d'appels directs avec nom et numéro de téléphone dans le système. Ces destinations doivent ensuite être attribuées uniquement par l'utilisateur aux appareils terminaux via l'interface de configuration de l'utilisateur. L'utilisateur peut ensuite définir l'appel direct système ou un appel direct spécifiquement configuré pour l'appel terminal dans la configuration.

7.1.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Contrôle d'appel**->**Services sortants**->**Appel direct**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'entrée.
Numéro d'appel direct	Saisissez le numéro d'appel à composer automatiquement si aucun autre numéro n'a été composé pendant un certain laps de temps après avoir décroché le combiné.

7.1.2 Transfert des appels (AWS)

Le menu **Contrôle d'appel**->**Services sortants**->**Transfert des appels (AWS)** permet de configurer les transferts d'appels externes pour un abonné interne.

Vous ne vous trouvez momentanément pas au bureau, mais ne souhaitez manquer aucun appel. Grâce au transfert des appels vers un autre numéro d'appel, p. ex. votre téléphone portable, vous pouvez répondre à vos appels, même lorsque vous n'êtes pas sur place. Vous pouvez dévier des appels vers le numéro d'appel de votre choix. Vous pouvez définir le paramètre *Immédiatement*, *En absence de réponse* ou *Si occupé*. Les déviations d'appels *En absence de réponse* et *Si occupé* peuvent coexister. Si, par exemple, votre téléphone ne se trouve pas à portée de main, l'appel est dévié vers un autre numéro d'appel (p. ex. votre téléphone portable) après un court laps de temps. Si vous êtes déjà en communication téléphonique sur votre lieu de travail, la ligne sera probablement « occupée » pour les autres appelants. La fonction de transfert des appels vous permet, en cas de ligne occupée, de rediriger ces appelants vers un collègue ou le secrétariat.

Chaque abonné interne du système peut transférer ses appels vers un autre numéro d'appel. Les appels peuvent être transférés vers des numéros d'appel d'abonnés internes, des numéros d'appel d'équipes internes ou des numéros d'appel externes. Lors de la saisie du numéro d'appel vers lequel vous souhaitez dévier les appels, le système vérifie automatiquement s'il s'agit d'un numéro d'appel interne ou externe.

Le transfert des appels peut être configuré pour un abonné d'une équipe. Cet appel continue à être signalé aux autres abonnés de l'équipe. Le transfert des appels vers un abon-

né interne ou externe est alors effectué dans le système.

Le transfert des appels vers un numéro d'appel interne est effectué dans le système. Si un appel interne doit être transféré vers un numéro d'appel externe, le transfert s'effectue également dans le système. La communication est alors établie via le groupage qui est activé pour l'abonné configuré. Si l'appel est transféré via une connexion RNIS, un canal B reste occupé, tandis que si un appel externe est transféré vers l'extérieur, les deux canaux B restent occupés. Deux possibilités existent pour le transfert d'un appel externe vers un numéro d'appel externe :

- Transfert des appels dans le central : le transfert des appels est effectué dans le central si, dans le cas d'un appel externe, seul un abonné interne est entré dans la répartition des appels. Pour transférer des appels dans le central, la fonctionnalité Call Deflection (connexion multi-appareils) ou Partial Rerouting (connexion de l'installation) doit être activée pour les connexion RNIS concernées dans le cas d'un fournisseur réseau.
- Transfert des appels dans le système : le transfert des appels est effectué dans le système si les fonctionnalités nécessaires pour le transfert des appels dans le central ne sont pas disponibles pour les connexions RNIS concernées. Si un appel externe est dirigé vers plusieurs téléphones (p. ex. une équipe) et que le transfert des appels a été configuré pour certains d'entre eux, le transfert en question est effectué dans le système. La communication externe est alors établie via le canal B d'un groupage, lequel est activé pour l'abonné configuré. Ce canal B reste occupé pour la durée d'un transfert d'appel actif.

Note

S'il est raccordé au RNIS externe, le système tente généralement de transférer les appels via le central dans le cas de communications de l'extérieur vers l'extérieur. Pour les équipes, il est possible de définir manuellement dans la configuration si les appels doivent être transférés via le central ou le système. Si le système ne dispose d'aucune connexion RNIS ou si la fonctionnalité Call Deflection (connexion multi-appareils) ou Partial Rerouting (connexion de l'installation) n'est pas active dans le cas d'un fournisseur réseau, les appels sont transférés uniquement dans le système.

7.1.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Contrôle d'appel**->**Services sortants**->**Transfert des appels (AWS)**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Numéro d'appel interne	Sélectionnez le numéro d'appel interne pour lequel les appels entrants doivent être transférés.
Type de la transmission de l'appel'	Indiquez le moment auquel les appels entrants doivent être déviés vers le numéro d'appel interne entré. Valeurs possibles : • *Immédiatement* • *Si occupé* • *En absence de réponse* (valeur par défaut) • *Si occupé / en absence de réponse*
Numéro d'appel de destination "en absence de réponse"	Saisissez le numéro d'appel vers lequel les appels entrants doivent être déviés en cas d'absence de réponse.
Numéro d'appel de destination "si occupé"	Saisissez le numéro d'appel vers lequel les appels entrants doivent être transférés en cas de ligne occupée.
Numéro d'appel de destination "immédiatement"	Saisissez le numéro d'appel vers lequel les appels entrants doivent être immédiatement déviés.

7.1.3 Contrôle de numérotation

Le menu **Contrôle d'appel**->**Services sortants**->**Contrôle de numérotation** permet de bloquer ou d'activer certains numéros d'appels/numéros d'appel d'abonnés.

Vous souhaitez éviter la numérotation de certains numéros d'appel dans le système, p. ex les numéros d'appel coûteux. Répertoriez ces numéros d'appel ou numéros d'appel d'abonnés dans la liste des numéros d'appel bloqués du contrôle de numérotation. Les abonnés soumis au contrôle de numérotation ne peuvent pas composer ces numéros d'appel. S'ils ont malgré tout besoin de certains numéros d'appel issus d'une zone bloquée, vous pouvez les activer via la liste des numéros d'appel activés du contrôle de numérotation.

A l'aide de la liste des numéros d'appel bloqués, vous pouvez bloquer certains numéros d'appel ou indicatifs. A l'aide de la liste des numéros d'appel activés, vous pouvez activer

certains numéros d'appel ou indicatifs bloqués. Si un numéro d'appel entré comme numéro d'appel activé est plus long qu'un numéro d'appel entré comme numéro d'appel bloqué, il peut être composé. Lorsque vous composez un numéro d'appel, la numérotation est interrompue après le chiffre bloqué et la sonnerie « occupé » retentit. Dans les paramètres de l'utilisateur, vous pouvez attribuer individuellement à chaque utilisateur un contrôle de numérotation.

Exemple : numéro d'appel bloqué *01*, tous les numéros d'appel externes commençant par *01* sont bloqués. Numéro d'appel activé *012345*, la numérotation peut avoir lieu. Tous les numéros d'appel externes commençant par *012345* peuvent être composés. Si deux numéros d'appel identiques (même suite de chiffres et même nombre de chiffres, p. ex *01234* et *01234*) figurent à la fois dans la liste des numéros d'appel activés et la liste des numéros d'appel bloqués, le numéro d'appel n'est pas composé.

Note

Dans la liste des numéros d'appel activés, des abonnés disposant d'une autorisation de sortie partielle ou ne disposant d'aucune autorisation de sortie (qui ne possèdent pas d'autorisation de numérotation externe) sont autorisés à composer les numéros d'appel externes activés.

Veillez à ce que l'indicatif réseau local soit défini dans la configuration afin d'éviter que le numéro d'appel bloqué sur le réseau local ne soit ignoré lors de la numérotation de l'indicatif réseau local.

7.1.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Contrôle d'appel**->**Services sortants**->**Contrôle de numérotation**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Numéro d'appel bloqué	Saisissez le numéro à ne pas composer.
Numéro d'appel activé	Saisissez le numéro dont la numérotation doit être explicitement autorisée.

7.1.4 Numéro d'appel prioritaire

Le menu **Contrôle d'appel**->**Services sortants**->**Numéro d'appel prioritaire** permet de configurer des numéros d'appel avec certaines fonctions spéciales, telles que les fonctions d'appel d'urgence.

Dans la configuration de votre système, vous pouvez définir des numéros d'appel qui doivent être joignables en cas d'urgence. Si vous composez l'un de ces numéros d'appel prioritaires, le système le reconnaît et active automatiquement un canal B RNIS. Si les canaux B RNIS externes sont déjà occupés, un canal B RNIS est activé et la sonnerie « occupé » retentit pour les abonnés souhaitant entrer en communication. Les appels prioritaires en cours ne sont pas interrompus.

7.1.4.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Contrôle d'appel**->**Services sortants**->**Numéro d'appel prioritaire**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'entrée.
Numéro prioritaire	Saisissez le numéro qui peut également être composé si tous les canaux B du système sont occupés. Un canal B externe est alors interrompu pour cette communication et occupé par l'appel prioritaire. Les appels prioritaires en cours ne sont pas interrompus.

7.2 Règles de sélection

Le menu **Contrôle d'appel**->**Règles de sélection** permet de définir des routes supplémentaires pour la numérotation externe dans la configuration de l'occupation de la ligne. Vous pouvez définir des groupages actifs spécifiquement pour les utilisateurs en fonction du numéro d'appel composé pour des communications sortantes ou saisir de nouveaux fournisseurs avec leur indicatif d'accès réseau. Le routage se définit ensuite pour chaque zone créée individuellement pour chaque jour de la semaine.

7.2.1 Général

Le menu **Contrôle d'appel**->**Règles de sélection**->**Général** permet d'activer la fonction ARS (Automatic Route Selection) et de sélectionner le niveau de routage souhaité.

Le menu **Contrôle d'appel**->**Règles de sélection**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
ARS	Indiquez si la fonctionnalité ARS (Automatic Route Selection) doit être activée. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Niveau de routage	Indiquez si un transfert doit être effectué vers d'autres routes en cas de non-accessibilité d'un groupage ou fournisseur entré. Valeurs possibles : • *1 (pas de Fallback)* : si le fournisseur entré ou le groupage sélectionné (**Contrôle d'appel**->**Règles de sélection**->**Zones et routage**-> **Editer/Ajouter** -> **Lu-Di** ->**Niveau de routage 1**) n'est pas disponible, la connexion est interrompue. • *2* : si le fournisseur entré ou le groupage sélectionné (**Contrôle d'appel**->**Règles de sélection**->**Zones et routage**-> **Editer/Ajouter** -> **Lu-Di** ->**Niveau de routage 1**) n'est pas disponible, une tentative de connexion via la variante de routage supplémentaire (**Contrôle d'appel**->**Règles de sélection**->**Zones et routage**-> **Editer/Ajouter** -> **Lu-Di** ->**Niveau de routage 2**) est effectuée. • *3* (valeur par défaut) : si ni le fournisseur ni le groupage entrés (**Contrôle d'appel**->**Règles de sélection**->**Zones et routage**-> **Editer/Ajouter** -> **Lu-Di** ->**Niveau de routage 1** et **Niveau de routage 2**) ne sont disponibles, la connexion est établie via le fournisseur (**Numérotation**->**Classe d'autorisation**->**Ajouter**->**Configuration de base**->**Occupation de la ligne avec indicatif**) entré par défaut pour l'utilisateur.

7.2.2 Interfaces/Fournisseurs

Le menu **Contrôle d'appel**->**Règles de sélection**->**Interfaces/Fournisseurs** permet de saisir les routes ou les fournisseurs et leur indicatif d'accès réseau.

7.2.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Contrôle d'appel**->**Règles de sélection**->**Interfaces/Fournisseurs**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'entrée.
Mode de routage	Sélectionnez la procédure d'acheminement des numérotations externes. Valeurs possibles : • *Par défaut* (valeur par défaut) : selon la procédure standard, l'indicatif entré sous **Indicatif fournisseur** est composé lors d'une communication externe. • *Route* : la communication externe est établie via le groupage sélectionné dans **Route**.
Indicatif fournisseur	Saisissez le numéro d'appel à utiliser comme préfixe dans le cas d'un appel externe, p. ex. pour établir une communication via un fournisseur Call by Call.
Route	Uniquement si **Mode de routage** = *Route*. Sélectionnez le groupage par lequel une communication vers l'extérieur doit être établie.

7.2.3 Zones et routage

Le menu **Contrôle d'appel**->**Règles de sélection**->**Zones et routage** permet de définir les zones dans lesquelles des numéros doivent être composés à l'aide de routes ou de fournisseurs spécifiques.

La configuration des tableaux de routage s'effectue pour chacune des zones définies et pour chaque jour de la semaine. Pour les deux tableaux de routage, les niveaux de routage 1 et 2 peuvent être définis comme Fallback.

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

7.2.3.1 Numéros d'appel

Dans la zone **Numéros d'appel**, saisissez les numéros d'appel ou les numéros d'appel d'abonnés pour lesquels vous souhaitez configurer des tableaux de routage.

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'entrée.
Zones	Configurez les zones externes vers lesquelles des numéros doivent être composés via les routes ou fournisseurs saisis. Valeurs possibles : • *Numéro d'appel / Numéro d'appel de l'abonné*: saisissez l'intégralité ou une partie du numéro d'appel qui désigne une zone. • *Nom*: Saisissez un nom pour cette zone.

7.2.3.2 Lu - Di

Dans la zone **Lu** - **Di**, sélectionnez les heures souhaitées pour chaque niveau de routage ainsi que la route ou le fournisseur de votre choix qui doit acheminer les appels sortants à partir de l'heure entrée.

Champs du menu <Jour de la semaine>

Champ	Description
Niveau de routage 1	Configurez les temps de commutation pour le niveau de routage 1. Pour ce faire, choisissez d'abord l' **Heure de début** à partir de laquelle acheminer les appels via une interface ou un fournisseur réseau spécifique, que vous pouvez sélectionner sous **Interface/Fournisseur réseau**.
Niveau de routage 2	Configurez les temps de commutation pour le niveau de routage 2. Pour ce faire, choisissez d'abord l' **heure de début** à partir de laquelle acheminer les appels via une interface ou un fournisseur réseau spécifique, que vous pouvez sélectionner sous **Interface/Fournisseur réseau**.

Chapitre 8 Applications

Vous pouvez configurer les fonctionnalités internes des téléphones du système sous **Applications**.

8.1 Calendrier

Le menu **Applications**->**Calendrier** permet de déterminer si de nouvelles entrées peuvent être créées ou si des modifications peuvent être effectuées dans le calendrier.

Chaque entreprise dispose d'horaires d'ouverture fixes. Vous pouvez enregistrer ces horaires dans les calendriers internes du système. Ainsi, tous les appels ayant lieu en dehors des heures d'ouverture peuvent être signalés à un poste d'opératrice ou un répondeur, par exemple. Pendant ce temps, vos collaborateurs peuvent accomplir d'autres tâches, sans être interrompus par des appels téléphoniques. Les différentes variantes d'appel d'une équipe sont automatiquement commutées par les calendriers.

Imaginons que vous souhaitiez modifier les autorisations concernant les communications externes après l'heure de fermeture pour certains abonnés. Dans la configuration du système, vous pouvez déterminer individuellement pour chaque utilisateur si l'autorisation de communication externe doit être commutée automatiquement. La commutation a lieu conformément aux données saisies dans le calendrier correspondant.

Vous pouvez définir cinq types de calendriers dans le système. Les calendriers « Classe d'autorisation » et « Service de nuit » sont prévus pour des commutations centralisées et ne peuvent être configurés qu'une seule fois. Les calendriers « Signalisation groupée », « Signalisation TFE » et « Rejet vers un numéro d'appel interne/externe » peuvent être configurés plusieurs fois. Plusieurs temps de commutation différents peuvent être sélectionnés pour chaque jour de la semaine.

Dans la configuration, vous pouvez affecter un calendrier à toutes les fonctionnalités pour lesquelles plusieurs variantes peuvent être définies (p. ex. équipes). La commutation entre les différentes variantes d'appel a alors lieu aux heures indiquées dans le calendrier affecté.

8.1.1 Calendrier

Le menu **Applications**->**Calendrier**->**Calendrier** permet d'afficher, de modifier ou de copier un calendrier déjà configuré, ainsi que de créer de nouveaux calendriers.

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

8.1.1.1 Général

La zone **Général** permet de définir le nom du calendrier à créer.

Le menu **Applications**->**Calendrier**->**Calendrier**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le calendrier.
Application	Déterminez pour quelle application le calendrier doit être utilisé. Notez que ce champ ne peut pas être modifié pour les entrées existantes. Si vous souhaitez configurer une autre application, vous devez créer une nouvelle entrée et supprimer l'entrée existante. Valeurs possibles : • *Signalisation groupée* (valeur par défaut) : vous pouvez configurer plusieurs calendriers ici. • *Signalisation TFE* : vous pouvez configurer plusieurs calendriers ici. • *Service de nuit* : un seul calendrier peut être configuré ici. • *Classe d'autorisation* : un seul calendrier peut être configuré ici. • *Rejet vers un numéro d'appel interne/externe* : vous pouvez configurer plusieurs calendriers ici. • *Système boîte vocale* : vous pouvez configurer plusieurs calendriers ici. • *Entrée d'alarme* : vous pouvez configurer plusieurs calendriers ici.

8.1.1.2 Lu - Di

Lu - Di

La zone **Lu - Di** permet de définir les jours et heures de commutation pour ce calendrier.

Le menu **Applications**->**Calendrier**->**Calendrier**->**Lu - Di** se compose des champs suivants :

Champs du menu <Jour de la semaine>

Champ	Description
Temps de commutation	Saisissez les temps de commutation souhaités. Sous **Heure**, sélectionnez pour chaque jour de la semaine les temps de commutation souhaités, auxquels il faut passer d'une variante de commutation active à la variante de commutation sélectionnée sous **Action**. Les variantes de commutation suivantes sont disponibles en fonction de l'utilisation : • *Signalisation groupée* : variante d'appel 1 à variante d'appel 4 • *Signalisation TFE* : variante d'appel TFE 1 et variante d'appel TFE 2 • *Service de nuit* : service de nuit actif et service de nuit inactif • *Classe d'autorisation* : classe d'autorisation par défaut et classe d'autorisation option • *Rejet vers un numéro d'appel interne/externe* : variante de rejet 1 à variante de rejet 4 • *Système boîte vocale* : action au bureau et à distance • *Entrée d'alarme* : service de nuit actif et service de nuit inactif.
Reprendre les paramètres de	Uniquement si des paramètres ont déjà été définis pour un jour de la semaine. Indiquez le jour de la semaine dont vous souhaitez reprendre les paramètres. Si vous avez besoin de paramètres précis pour ce jour de la semaine, sélectionnez l'option *Individuel*.

8.1.1.3 Exception

Dans la zone **Exception**, indiquez si et comment il faut tenir compte des jours fériés.

Le menu **Applications**->**Calendrier**->**Calendrier**->**Exception** se compose des champs suivants :

Champs du menu Paramètres jours fériés

Champ	Description
Prendre en compte les jours fériés	Indiquez s'il faut également tenir compte des délais enregistrés dans le menu **Applications**->**Calendrier**->**Jours fériés** dans ce calendrier. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Reprendre les paramètres de	Uniquement si **Prendre en compte les jours fériés** est activé. Indiquez le jour de la semaine dont vous souhaitez reprendre les paramètres relatifs aux jours fériés. Le menu **Applications**->**Calendrier**->**Calendrier**->**Lu - Di** permet de configurer les jours de la semaine. Si vous avez besoin de paramètres précis pour les jours fériés, sélectionnez l'option *Individuel*.
Temps de commutation	Uniquement pour **Reprendre les paramètres de** = *Individuel*. Saisissez les temps de commutation souhaités. Sous **Heure**, sélectionnez les temps de commutation souhaités, auxquels il faut passer d'une variante de commutation active à la variante de commutation sélectionnée sous **Action**. Les variantes de commutation suivantes sont disponibles en fonction de l'utilisation : • *Signalisation groupée* : variante d'appel 1 à variante d'appel 4 • *Signalisation TFE* : variante d'appel TFE 1 et variante d'appel TFE 2 • *Service de nuit* : service de nuit et service de nuit inactif • *Classe d'autorisation* : classe d'autorisation par défaut et classe d'autorisation option

Champ	Description
	• *Rejet vers un numéro d'appel interne/externe* : variante de rejet 1 à variante de rejet 4 • *Système boîte vocale* : action au bureau et à distance • *Entrée d'alarme* : service de nuit actif et service de nuit inactif.

8.1.2 Jours fériés

Le menu **Applications**->**Calendrier**->**Jours fériés** permet d'entrer des jours fériés ou d'autres jours spéciaux lors desquels des paramètres différents doivent être activés via le calendrier. Les entrées de jours fériés sont triées par date.

8.1.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Applications**->**Calendrier**->**Jours fériés**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le jour férié.
Date (JJ-MM)	Saisissez la date avec le jour et le mois en utilisant deux chiffres. Les entrées incorrectes, p. ex. le 31.02., sont acceptées et enregistrées, mais ne sont pas exécutées par le système.

8.2 Rejet

Le menu **Applications**->**Rejet** permet de configurer la procédure par défaut à appliquer pour les appels entrants dans le système.

8.2.1 Fonctions de rejet

Le menu **Applications**->**Rejet**->**Fonctions de rejet** permet de définir différentes variantes de rejet pour *Direct*, *Si occupé*, *En absence de réponse* ou *Si occupé et en absence de réponse*. Vous pouvez ensuite affecter ces variantes de rejet aux connexions externes dans le menu **Numérotation**->**Répartition des appels**->**Affectation des appels**.

8.2.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des variantes de rejet.

Le menu **Applications**->**Rejet**->**Fonctions de rejet**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour la fonction de rejet.
Type de la fonction de rejet	Sélectionnez la fonction de transmission souhaitée. Valeurs possibles : • *Direct* (valeur par défaut) • *Si occupé* • *En absence de réponse* • *Si occupé et en absence de réponse*

Champs du menu Paramètres si occupé

Champ	Description
Nombre d'abonnés dans la boucle d'attente	Uniquement pour le type **de la fonction de rejet** = *Si occupé* ou *Si occupé et en absence de réponse* : Ce champ vous permet de définir le nombre maximal d'abonnés dans la file d'attente. La file d'attente peut compter jusqu'à 10 abonnés. Les autres appelants entendent le signal « occupé ». Les valeurs possibles sont comprises entre *0* (aucune file

Champ	Description
	d'attente) et *10*. La valeur par défaut est *0*.
Accepter les appel en attente avec	Uniquement pour le type **de la fonction de rejet** = *Si occupé* ou *Si occupé et en absence de réponse* : Déterminez ce que les appelants de la file d'attente entendent (musique d'attente interne ou configurée, annonce). Valeurs possibles : • *MoH Wave 1* à *MoH Wave 8* • *MoH Intern 1* (valeur par défaut) • *MoH Intern 2* • *Arrêt*
Temps d'attente maxi dans la boucle d'attente	Uniquement pour le type **de la fonction de rejet** = *Si occupé* ou *Si occupé et en absence de réponse* : Définissez la durée maximale qu'un appelant peut passer dans la file d'attente. Une fois ce délai écoulé, l'appelant est transmis à la destination de rejet définie. Laissez le paramètre *Sans fin* pour une file d'attente sans fin (correspond à la valeur 0). Désactivez le paramètre *Sans fin* afin de pouvoir saisir la valeur souhaitée.

Champs du menu Paramètres en absence de réponse

Champ	Description
Heure de reroutage en cas d'absence de réponse	Définissez la durée maximale qu'un appelant peut passer dans la file d'attente lorsqu'il n'arrive pas à joindre le numéro d'appel de destination. Une fois ce délai écoulé, l'appelant est transmis à la destination de rejet définie. La valeur par défaut est *30* secondes.

Champs du menu Autres paramètres

Champ	Description
Annonce	Déterminez si l'appel entrant doit être rejeté avec une annonce. Valeurs possibles : • *Arrêt* (valeur par défaut) : l'appel entrant n'est pas rejeté

Champ	Description
	avec une annonce. • *MoH Wave 1* à *MoH Wave 8*
Numéro d'appel de destination	Sélectionnez le numéro d'appel interne vers lequel l'appel entrant doit être renvoyé. Valeurs possibles : • *Pas de numéro d'appel (coupure de ligne)* : la connexion et l'appel sont interrompus. • *<Numéro d'appel>* : si un numéro d'appel de destination est défini, un transfert a lieu.
Transmettre avec	Pendant le transfert de son appel, l'appelant entend l'annonce ou la musique définie ici. Valeurs possibles : • *Tonalité* • *MoH Wave 1* à *MoH Wave 8* • *MoH Intern 1* • *MoH Intern 2* • *<Fichier wave>*

Annonce avant interrogation

Vous avez mis en place un numéro général d'information que les clients appellent pour faire part de demandes et de problèmes divers. Un collaborateur ou une équipe ne peut évidemment pas les renseigner sur tous les sujets. L'appelant doit alors être redirigé vers les services spécialisés. Si vous connaissiez la demande d'un appelant avant, vous pourriez le transférer directement vers le service approprié. De cette manière, cela évite à vos clients de devoir d'abord être pris en charge par un poste d'opératrice, puis seulement transférés. Chaque appelant décide lui-même du collaborateur / de l'interlocuteur avec lequel il souhaite être mis en relation.

Avec la fonctionnalité **Annonce avant interrogation avec DISA**, les appels sont automatiquement acceptés par le système. L'appelant entend une annonce lui indiquant les saisies possibles pendant ou après l'annonce. Une fois la saisie effectuée, l'annonce prend fin et l'appelant est transféré vers une équipe ou un abonné interne. Si l'appelant n'effectue aucune saisie ou si la saisie est erronée, il est transféré vers la destination de rejet définie (équipe ou abonné interne). Pendant le transfert, l'appelant entend la tonalité ou une musique d'attente du système.

Note

DISA - Direct Inward System Access. Une fois un appel accepté par le système, l'appelant est automatiquement transféré après la saisie d'un code. Ce code est affecté à un numéro d'appel interne dans le système. La saisie d'un numéro d'appel ou d'un code doit avoir lieu pendant l'annonce. Si l'annonce (fichier wave) est déjà terminée, aucune saisie n'est plus prise en compte. Un renvoi a alors lieu vers la destination de rejet définie. La fonctionnalité **Annonce avant interrogation avec DISA** fait partie du système et permet d'accepter jusqu'à 28 appels en même temps.

Champs du menu Annonce/Paramètres de l'Auto Attendant

Champ	Description
Transmission	Déterminez la manière dont un appel entrant doit être transmis. Valeurs possibles : • *Annonce sans DISA* (valeur par défaut) : l'annonce configurée est lue. Ensuite, le transfert est effectué vers le numéro d'appel interne configuré, ou la connexion est interrompue et l'appelant entend la sonnerie « occupé ». • *DISA, les numéros d'appel internes sont composés* : l'appelant est invité à saisir un numéro d'appel interne. Le transfert est alors effectué. • *DISA, les numéros de code sont composés* : l'appelant est invité à saisir un code compris entre 0 et 9. Les codes sont affectés aux numéros d'appel internes souhaités. L'appelant est finalement transféré vers le numéro d'appel interne configuré.
Nombre d'émissions	Déterminez le nombre de fois consécutives que l'annonce doit être répétée. Ensuite, l'appelant entend la sonnerie « occupé ».
Annonce avant interrogation avec DISA	Uniquement si **Transmission** = *DISA, les numéros de code sont composés* Pour chaque code DISA, sélectionnez le numéro d'appel interne souhaité vers lequel l'appelant doit être transféré.

8.2.2 Applications du rejet

Le menu **Applications**->**Rejet**->**Applications du rejet** permet de configurer les moments où chaque variante de rejet doit être activée. Vous pouvez commuter les différentes variantes manuellement ou via un calendrier.

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des applications de rejet.

8.2.2.1 Général

La zone **Général** permet d'effectuer les paramétrages de base d'une application de rejet.

Le menu **Applications**->**Rejet**->**Applications du rejet**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour l'application de rejet.
Type de l'application de rejet	Sélectionnez la destination vers laquelle un appel entrant doit être renvoyé. Valeurs possibles : • *Numéro d'appel de la connexion* (valeur par défaut) • *Abonné interne* • *Global*
Commuter la variante d'appel	Déterminez la manière dont la commutation entre les variantes doit avoir lieu. Valeurs possibles : • *Pas de calendrier, uniquement manuel* • *<Calendrier>*

8.2.2.2 Variante 1 - 4

La zone **Variante** permet de définir les variantes de rejet. Vous pouvez configurer jusqu'à quatre variantes.

Le menu **Applications**->**Rejet**->**Applications du rejet**->**Variante** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Affectation	Sélectionnez la fonction de rejet à laquelle vous souhaitez affecter la variante sélectionnée.

8.3 Application vocale

Le menu **Applications**->**Application vocale** permet de configurer les fichiers wave de votre système.

Une prise en charge professionnelle par téléphone fait déjà office de carte de visite pour une entreprise. Les applications vocales permettent à chaque entreprise de se démarquer. En outre, pendant le transfert, l'appelant peut être informé ou simplement diverti par une musique d'attente agréable (ces paramètres peuvent également être différents en fonction du service, p. ex.).

Imaginons que vous vouliez utiliser vos propres annonces ou une musique particulière comme musique d'attente pour vos clients. Vous pouvez diffuser des fichiers wave créés par vos soins dans le système.

Vous pouvez enregistrer des fichiers musicaux ou vocaux personnalisés dans le système. La configuration de base du système permet de stocker 2 mélodies MoH. En utilisant une carte SD, vous pouvez augmenter la capacité de mémoire disponible. La taille des fichiers musicaux et vocaux pouvant être enregistrés dépend de la capacité de la carte SD utilisée. Les fichiers sont enregistrés au format wave.

Les applications vocales suivantes peuvent être configurées dans le système :

- Annonce avant interrogation
- Annonce sans interrogation/Infobox
- Signal d'alerte
- Musique d'attente/Music on Hold

Des informations supplémentaires quant au fonctionnement, à la configuration et à l'utilisation sont disponibles dans la description des différentes fonctionnalités.

Configurations de base des applications vocales

Les applications vocales peuvent être affectées aux fonctionnalités de deux manières différentes.

Tous les utilisateurs qui se servent d'une application vocale avec ce circuit de connexion entendent toujours la musique ou l'annonce vocale correspondante depuis le début. Un utilisateur supplémentaire entend la musique ou l'annonce vocale depuis le début. Le nombre d'utilisateurs simultanés d'une telle application vocale est limité à 28.

Veillez à ce que la musique lue pour l'extérieur et les musiques de l'application vocale soient exemptes de droits de tiers. Avant d'être enregistrés sur le système, les fichiers existants dans un autre format doivent être convertis au format wave spécifique à l'entreprise.

Note

Notez que les fichiers wave doivent se présenter au format suivant :

- Débit binaire : 128 kbit/s
- Taille de l'échantillon : 16 bits
- Canaux : 1 (mono)
- Fréquence d'échantillonnage : 8 kHz
- Format audio : PCM

8.3.1 Fichiers wave

Le menu **Applications**->**Application vocale**->**Fichiers wave** permet de charger vos fichiers d'annonce/de mélodie et de régler le volume. Vous avez en outre la possibilité d'écouter des messages vocaux ou de les télécharger sur votre PC. Cliquez sur le symbole pour enregistrer un message. La boîte de dialogue de téléchargement s'ouvre ensuite. Cliquez sur le symbole pour écouter le message vocal.

8.3.1.1 Editer

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez pour supprimer une entrée existante.

Les paramètres *MoH Intern 1* et *MoH Intern 2* sont des fichiers prédéfinis dans le système, et ne peuvent dès lors pas être supprimés.

Le menu **Applications**->**Application vocale**->**Fichiers wave**->**Editer** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour le fichier wave.
Sélectionner le fichier	Cliquez sur l'option **Parcourir...** et, dans la fenêtre de l'explorateur, sélectionnez le fichier wave qui doit être chargé dans le système.
Volume	Sélectionnez le volume de lecture par défaut du fichier wave. Sélectionnez *0* pour lire le fichier avec un volume prédéfini. Les valeurs négatives vous permettent de diminuer progressivement le volume, les valeurs positives de l'augmenter. Valeurs possibles : • *-5* • *-4* • *-3* • *-2* • *-1* • *0* (valeur par défaut) • *+1* • *+2* • *+3*

8.4 Répertoire téléphonique du système

Le menu **Applications**->**Répertoire téléphonique du système** permet d'entrer des numéros d'appel dans le répertoire téléphonique du système et de les gérer.

Les collaborateurs de votre entreprise doivent entrer en contact téléphonique avec de nombreux clients. C'est ici que le répertoire téléphonique du système trouve son utilité. Celui-ci leur permet de ne pas devoir saisir le numéro d'appel du client : il leur suffit de sélectionner le nom sur l'écran du téléphone système pour lancer la numérotation. Les noms et numéros de téléphone des clients peuvent être gérés de manière centralisée par un collaborateur. Si un client faisant partie du répertoire téléphonique appelle, son nom s'affiche sur l'écran du téléphone système. Le système dispose d'un répertoire téléphonique intégré, dans lequel vous pouvez enregistrer des numéros comportant 24 chiffres maximum et des noms comportant 20 caractères maximum.

Une **Numérotation abrégée** est affectée à chaque entrée créée dans le répertoire téléphonique. Le numéro abrégé permet aux téléphones autorisés de réaliser une numérotation abrégée depuis le répertoire téléphonique.

Téléphones système

Les téléphones système peuvent effectuer une numérotation via un menu particulier du répertoire téléphonique du système. Pour rechercher une entrée du répertoire téléphonique, saisissez les premières lettres (8 maximum) du nom souhaité et confirmez la saisie. Huit entrées du répertoire téléphonique du système sont toujours mises à votre disposition. Vous pouvez les voir les unes après les autres. Sélectionnez l'entrée souhaitée, puis confirmez à l'aide du bouton **OK**. Vous devez lancer la numérotation dans un délai de 5 secondes. Dans la liste de rappel du téléphone système, le nom de l'abonné sélectionné s'affiche, plutôt que son numéro. Si un téléphone système reçoit un appel d'une entrée enregistrée dans le répertoire téléphonique du système, l'écran du téléphone système affiche le nom de l'appelant.

Note

Les numéros d'appel supplémentaires d'un utilisateur (**Numéro de mobile** et **Numéro d'appel privé**) n'apparaissent que dans le menu du répertoire téléphonique du téléphone système. Ils ne s'affichent pas dans le menu **Répertoire téléphonique du système** de l'interface utilisateur. Les entrées du menu de répertoire téléphonique du téléphone système avec la mention (M) indiquent un **Numéro de mobile** d'un utilisateur. La mention (H) indique quant à elle un **Numéro d'appel privé**.

Note

L'appareil **hybird** prend en charge le protocole LDAP (Lightweight Directory Access Protocol) afin de mettre les entrées du répertoire téléphonique du système à la disposition d'autres appareils ou systèmes. Le nom, le numéro d'appel (MSN) ainsi que les numéros d'appel mobiles et privés peuvent ainsi être transférés.

8.4.1 Entrées

Le menu **Applications**->**Répertoire téléphonique du système**->**Entrées** affiche toutes les entrées définies du répertoire téléphonique avec la numérotation abrégée correspondante. Dans la colonne **Description**, les entrées sont classées par ordre alphabétique. Vous pouvez cliquer sur le titre de la colonne de votre choix et trier les entrées dans l'ordre croissant ou décroissant.

8.4.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Applications**->**Répertoire téléphonique du système**->**Entrées**->**Nouveau** se compose des champs suivants :

Champs du menu Entrée du répertoire téléphonique

Champ	Description
Description	Saisissez une description pour l'entrée. Le tri ultérieur dans le répertoire téléphonique a lieu en fonction de la première lettre de l'entrée.
Numéro de téléphone	Saisissez le numéro de téléphone (interne ou externe).
Numérotation abrégée	Indiquez une numérotation abrégée. Si vous n'en saisissez aucune, une numérotation abrégée est affectée automatiquement. Les nombres possibles sont compris entre *0* et *999*.
Call Through	Indiquez si le numéro de téléphone doit être activé pour la fonction **Call Through**. Si tel est le cas et qu'un appelant utilise ce numéro pour la fonction **Call Through**, son autorisation est contrôlée à l'aide de l'entrée du répertoire téléphonique. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

8.4.2 Importation / Exportation

Le menu **Applications**->**Répertoire téléphonique du système**->**Importation / Exportation** permet d'importer et d'exporter les données de répertoire téléphonique. Vous pouvez, par exemple, importer des données exportées depuis Microsoft Outlook. Lors de l'exportation des données de répertoire téléphonique enregistrées sur votre appareil, un fichier texte est créé.

Le menu **Applications**->**Répertoire téléphonique du système**->**Importation / Exportation** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Action	Sélectionnez l'action souhaitée. Valeurs possibles : • *Exporter* (valeur par défaut) : vous pouvez exporter les noms (avec numéros de téléphone, numérotations abrégées, Call Through) enregistrés sous **Applications**->**Répertoire téléphonique du système**->**Entrées** dans un fichier texte. • *Importer* : vous pouvez importer un fichier texte au format suivant : le fichier à importer doit comporter des lignes individuelles au format description,numéro de téléphone,numérotation abrégée,Call Through (1 = activé, 2 = désactivé). Exemple : Name,Phone Number,Speeddial Number,Call Through Hans,123456,1,1 Klaus,234567,2,2 Max,345678,3,1
Séparateur	Uniquement pour **Action** = *Importer* et **Format de fichier par défaut** non *Activé* Indiquez le séparateur utilisé dans le fichier à importer. Valeurs possibles :

Champ	Description
	• *Virgule* (valeur par défaut) • *Point-virgule* • *Espace* • *Tabulateur*
Sélectionner le fichier	Uniquement pour **Action** = *Importer* Sélectionnez le fichier à importer.

Vous avez également la possibilité d'importer un fichier CSV.

Dans la mesure où le fichier comprend plusieurs colonnes, vous avez la possibilité de générer deux entrées de répertoire lors de l'importation (p. ex. une entrée professionnelle et une entrée privée). Lors d'une étape d'importation suivante, spécifiez pour ce faire les données qui doivent être reprises comme nom et numéro de téléphone. Si vous ne souhaitez générer qu'une entrée de répertoire, sélectionnez l'option vide dans tous les champs de la deuxième entrée **Importation annuaire téléphonique**.

Champs du menu Importation annuaire téléphonique

Champ	Description
Numéro de téléphone	Sélectionnez les données d'un fichier qui doivent être reprises comme numéro de téléphone.
Nom	Sélectionnez les colonnes d'un fichier qui doivent être reprises comme nom. Vous avez la possibilité d'importer deux éléments (p. ex. nom et prénom). Une chaîne de caractères peut être placée entre les deux éléments à l'aide du champ de saisie du milieu. Le séparateur par défaut est une virgule.

La numérotation abrégée est affectée automatiquement. La fonction Call Through est désactivée par défaut.

8.4.3 Général

Le menu **Applications**->**Répertoire téléphonique du système**->**Général** permet de définir le nom d'utilisateur et le mot de passe pour l'administration du répertoire téléphonique du système. La zone Répertoire téléphonique permet à l'administrateur d'afficher le répertoire téléphonique, de le modifier, d'importer et d'exporter des données.

Le menu **Applications**->**Répertoire téléphonique du système**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Nom de l'utilisateur pour accès web	Saisissez un nom d'utilisateur pour l'administrateur du répertoire téléphonique du système.
Mot de passe pour accès web	Saisissez un mot de passe pour l'administrateur du répertoire téléphonique du système.
Supprimer le répertoire téléphonique	Si vous souhaitez supprimer toutes les entrées du répertoire téléphonique existant du système, activez l'option **Supprimer**. La demande de confirmation suivante s'affiche : **Voulez-vous vraiment supprimer toutes les entrées du répertoire téléphonique ?** Confirmez votre saisie en cliquant sur **OK**.

8.5 Données de connexion

Le menu **Applications**->**Données de connexion** permet de configurer le relevé des connexions entrantes et sortantes.

Le relevé des données de connexion vous fournit un aperçu quant au comportement téléphonique de votre entreprise.

Toutes les communications externes peuvent être enregistrées dans l'appareil sous la forme de données de connexion. Ces données vous permettent de retrouver des informations importantes relatives aux différentes communications.

Vous devez activer le relevé des données de connexion dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Classes d'autorisation**->**Applications**. A la livraison, la fonction est désactivée.

8.5.1 Sortant

Le menu **Applications**->**Données de connexion**->**Sortant** contient des informations qui permettent de surveiller les activités sortantes.

Le menu **Applications**->**Données de connexion**->**Sortant** se compose des champs suivants :

Champs du menu Sortant

Champ	Description
Date	Permet d'afficher la date de la communication.
Heure	Permet d'afficher l'heure du début de la conversation.
Durée	Permet d'afficher la durée de la communication.
Utilisateur	Permet d'afficher l'appelant.
N° appel int.	Permet d'afficher le numéro d'appel interne de l'utilisateur.
Numéro d'appel composé	Permet d'afficher le numéro d'appel composé.
Numéro de projet	Permet d'afficher, le cas échéant, le numéro de projet de la conversation.
Interface	Permet d'afficher l'interface via laquelle la communication vers l'extérieur a été établie.
Coûts	Permet d'afficher les frais de communication, mais uniquement si le fournisseur transmet les informations correspondantes.

8.5.2 Entrant

Le menu **Applications**->**Données de connexion**->**Entrant** contient des informations qui permettent de surveiller les activités entrantes.

Le menu **Applications**->**Données de connexion**->**Entrant** se compose des champs suivants :

Champs du menu Entrant

Champ	Description
Date	Permet d'afficher la date de la communication.
Heure	Permet d'afficher l'heure du début de la conversation.
Durée	Permet d'afficher la durée de la communication.
Utilisateur	Permet d'afficher l'appelé.

Champ	Description
N° appel int.	Permet d'afficher le numéro d'appel interne de l'utilisateur.
Numéro d'appel externe	Permet d'afficher le numéro d'appel de l'appelant.
Numéro de projet	Permet d'afficher, le cas échéant, le numéro de projet de la conversation.
Interface	Permet d'afficher l'interface via laquelle la communication depuis l'extérieur a été établie.

8.5.3 Général

Le menu **Applications**->**Données de connexion**->**Général** permet de définir la manière dont les données de connexion sont enregistrées dans le système.

Le menu **Applications Données de connexion Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Nom de l'utilisateur pour accès web	Saisissez un nom d'utilisateur pour l'administrateur des données de connexion.
Mot de passe pour accès web	Saisissez un mot de passe pour l'administrateur des données de connexion.
Enregistrer les connexions sortantes	Sélectionnez les connexions sortantes qui doivent être enregistrées. Valeurs possibles : • *aucun* (valeur par défaut) • *Tous* • *Uniquement avec numéro de projet*
Enregistrer les connexions entrantes	Sélectionnez les connexions entrantes qui doivent être enregistrées. Valeurs possibles :

Champ	Description
	• *Aucune* (valeur par défaut) • *Tous* • *Uniquement avec numéro de projet*
Abréviation du numéro	Indiquez si le numéro d'appel doit être enregistré en abrégé. Si, pour des raisons de protection de données, l'affichage du numéro d'appel ne peut être que partiel, vous pouvez définir ici le nombre de caractères qui ne doivent pas s'afficher. Vous pouvez indiquer séparément le nombre de chiffres masqués pour les **Connexions sortantes** et les **Connexions entrant**. Le masquage des chiffres s'effectue de droite à gauche. Valeurs possibles : • *Non* (valeur par défaut) • *Tous* • *1* à *9*
Imprimer les données de connexion via Serial 2	Uniquement pour **hybird 300** / **hybird 600** Indiquez si les données de connexion de chaque communication doivent être transmises via l'interface série (Serial 2). De cette manière, vous pouvez connecter une solution logicielle externe pour la comptabilité des appels (application dans les hôtels). Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Champs du menu Actions

Champ	Description
Exporter les donnée de connexion	Si vous souhaitez enregistrer les données de connexion dans un fichier externe, cliquez sur l'option **Exporter** et enregistrez le fichier à l'emplacement souhaité, avec le nom de votre choix.
Supprimer les données de connexion	Si vous souhaitez supprimer les données de connexion de la mémoire du système, cliquez sur l'option **Supprimer**.

8.6 Centre d'appel mini

Le centre d'appel mini est une solution intégrée au système pouvant être utilisée par 16 agents maximum. Il s'agit d'une solution idéale pour les petits groupes qui utilisent les télécommunications de manière très dynamique (p. ex. service commercial, service d'assistance, acceptation/traitement des tâches, service après-vente). Une solution propre avec un administrateur spécifique a ici été intégrée au système. Le centre d'appel mini présente les caractéristiques suivantes :

- Attribution flexible des agents et des lignes.
- Adaptation dynamique en fonction du volume d'appels.
- Répartition des appels avec des périodes de repos pour l'agent.
- Données statistiques relatives aux agents et aux lignes.

8.6.1 État

Le menu **Applications**->**Centre d'appel mini**->**État** permet d'afficher l'état des lignes et des agents connectés, ainsi que les abonnés affectés aux lignes, et ce, en un seul bloc.

Le menu **Applications**->**Centre d'appel mini**->**État** se compose des champs suivants :

Valeurs de la liste État

Champ	Description
Aperçu	Le champ **Aperçu** permet de déterminer quels centres d'appel afficher.
Ligne	Permet d'afficher la ligne du centre d'appel mini.
Agents affectés	Permet d'afficher le nombre d'agents auxquels cette ligne est affectée.
Agents connectés	Permet d'afficher le nombre d'agents connectés à cette ligne.
Agents en post-traitement	Permet d'afficher le nombre d'agents qui se trouvent en post-traitement.
Appels actifs	Permet d'afficher le nombre de connexions actives.
Appel en attente	Permet d'afficher le nombre d'appels entrants en attente.

Champ	Description
Appels reçus aujourd'hui	Permet d'afficher le nombre d'appels reçus ce jour-là.
Appels manqués aujourd'hui	Permet d'afficher le nombre d'appels manqués ce jour-là.

8.6.2 Lignes

Dans le menu **Applications**->**Centre d'appel mini**->**Lignes**, les lignes sont affectées aux numéros d'appel internes et externes, et le nom du centre d'appel auquel appartient la ligne s'affiche.

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

8.6.2.1 Général

La zone **Général** vous permet d'effectuer les paramétrages de base d'une ligne.

Le menu **Applications**->**Centre d'appel mini**->**Lignes**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Saisissez une description pour la ligne.
Numéro d'appel externe	Sélectionnez l'un des numéros d'appel configurés comme centre d'appel mini pour la connexion externe de cette ligne de centre d'appel.
Numéro d'appel interne	Saisissez le numéro d'appel interne de votre choix pour cette ligne.
Description du centre d'appel	Sélectionnez l'option *Nouveau* et saisissez un nom pour le nouveau centre d'appel mini. Vous pouvez également sélectionner le nom d'un centre d'appel mini existant.

Champs du menu Autres paramètres

Champ	Description
Commuter la variante d'appel	Indiquez si les variantes d'appel pour cette ligne doivent être commutées via un calendrier configuré et, si tel est le cas, lequel. Valeurs possibles : • *Pas de calendrier, uniquement manuel* • *<Calendrier>*
Variante d'appel active	Sélectionnez la variante d'appel qui doit être activée par défaut pour cette ligne après la configuration.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Temps de franchissement	Indiquez la durée après laquelle un appel doit être transféré vers l'agent libre suivant qui est affecté à cette ligne.

8.6.2.2 Variante 1 - 4

La zone **Variante** vous permet de définir les variantes d'appel du centre d'appel mini.

Le menu **Applications**->**Centre d'appel mini**->**Lignes**->**Variante** se compose des champs suivants :

Champs du menu Paramètres

Champ	Description
Prise d'appel automatique avec	Indiquez si un appel entrant doit être accepté automatiquement et, si tel est le cas, avec quelle annonce ou mélodie. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Sélectionnez le fichier wave à utiliser pour la prise d'appel. Vous pouvez sélectionner tous les fichiers wave prédéfinis dans le système, ainsi que les fichiers supplémentaires qui y sont chargés.

Champs du menu Fonctions de rejet

Champ	Description
Rejet en absence de réponse	Indiquez si un appel entrant doit être renvoyé après une durée définie et, si tel est le cas, avec quelle variante. Valeurs possibles : • *aucun* : aucun renvoi ne doit avoir lieu en cas d'absence de réponse. • *<Equipe>* : l'appel entrant est transféré à l'équipe sélectionnée après la durée spécifiée sous **Temps avant rejet**.
Autres fonctions de rejet	Sélectionnez d'autres fonctions de rejet. Vous devez d'abord les configurer sous **Applications**->**Rejet**->**Fonctions de rejet**. Ensuite, vous avez la possibilité de sélectionner les valeurs suivantes : • *Arrêt* : aucune autre fonction de rejet. • *Immédiatement* : permet de transférer l'appel immédiatement, selon une fonction de rejet configurée. • *Si occupé* : permet de transférer l'appel lorsque la ligne est occupée, selon une fonction de rejet configurée.
Fonction de rejet	Uniquement pour **Autres fonctions de rejet** = *Immédiatement* ou **Autres fonctions de rejet** = *Si occupé* Sélectionnez une variante de rejet configurée pour le rejet « immédiatement » ou le rejet « si occupé ».
Occupé quand	Uniquement pour **Autres fonctions de rejet** = *Si occupé* Indiquez à partir de quel nombre d'agents occupés la ligne doit être considérée comme occupée.

8.6.2.3 Ouverture/fermeture de session

Dans la zone **Ouverture/fermeture de session**, sélectionnez les agents affectés à la ligne qui doivent être connectés.

Le menu **Applications**->**Centre d'appel mini**->**Lignes**->**Ouverture/fermeture de session** se compose des champs suivants :

Champs du menu Ouverture/fermeture de session

Champ	Description
Numéros d'appel	Permet d'afficher le numéro d'appel interne et la description de l'agent affecté.
État	Indiquez si l'agent est connecté à la ligne. Sélectionnez *Connecté* pour connecter l'agent.

8.6.3 Agents

Le menu **Applications**->**Centre d'appel mini**->**Agents** permet d'affecter les lignes aux agents. Un agent peut utiliser une ou plusieurs lignes de centre d'appel mini.

8.6.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Applications**->**Centre d'appel mini**->**Agents**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Utilisateur	Sélectionnez l'utilisateur configuré qui doit travailler en tant qu'agent du centre d'appel. Vous pouvez configurer l'utilisateur nécessaire dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**.
Numéro d'appel interne	Sélectionnez le numéro d'appel interne de l'utilisateur qui doit être utilisé pour le centre d'appel.

Champs du menu Lignes affectées

Champ	Description
Sélectionner les lignes	Sélectionnez les lignes desquelles l'agent doit être responsable. Lors de la sélection des lignes, le nom du centre d'appel correspondant est encore affiché afin de fournir un meilleur aperçu. Sous **Affecter**, indiquez si l'entrée doit être activée.

Champs du menu Réglages Post-traitement

Champ	Description
Post-traitement	Indiquez le temps dont cet agent dispose pour le post-traitement après une conversation téléphonique. Pendant ce temps, aucune nouvelle communication ne peut être affectée à l'agent. L'agent a la possibilité d'augmenter temporairement cette durée grâce à une procédure téléphonique.

8.6.4 Général

Le menu **Applications**->**Centre d'appel mini**->**Général** permet de configurer un accès aux interfaces Web HTML pour le gestionnaire du centre d'appel mini. Il peut alors contrôler l'état des lignes et des agents, et modifier leurs paramètres.

Le menu **Applications**->**Centre d'appel mini**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Nom de l'utilisateur pour accès web	Saisissez un nom d'utilisateur pour l'administrateur du centre d'appel mini. Lorsqu'un utilisateur se connecte avec ce nom à l'interface utilisateur, il a accès à l'interface utilisateur avec les paramètres sélectionnés pour la gestion du centre d'appel.
Mot de passe pour accès web	Saisissez un mot de passe pour l'administrateur du centre d'appel mini.

8.7 Adaptateur TFE

Vous pouvez connecter un dispositif d'ouverture de porte main-libre sous forme d'adaptateur TFE à une connexion analogique de votre système.

Si un adaptateur TFE est connecté à votre système, vous pouvez parler avec un visiteur se trouvant à la porte depuis n'importe quel téléphone autorisé. Vous pouvez affecter chaque sonnerie à certains téléphones, qui sonnent alors lorsque cette touche de sonnerie est activée. Sur les téléphones analogiques, la signalisation s'effectue en fonction de l'appel du portier. Plutôt que de configurer des téléphones internes, vous pouvez également configurer un téléphone externe comme destination d'appel pour la touche de sonnerie. Votre portier peut comporter jusqu'à 4 touches de sonnerie. Le dispositif électrique

d'ouverture de porte peut être activé pendant une conversation avec une personne se trouvant à la porte. Il ne peut pas être activé sans conversation.

Note

Toutes les fonctions du dispositif d'ouverture de porte main-libre (adaptateur TFE) sont commandées grâce aux codes indiqués dans le mode d'emploi du TFE. Le système ne prend pas en charge le TFE avec ses propres codes.

8.7.1 Adaptateur TFE

Le menu **Applications**->**Adaptateur TFE**->**Adaptateur TFE** permet de sélectionner la connexion analogique interne (FXS) à laquelle un adaptateur TFE doit être connecté. Vous pouvez, en outre, sélectionner le numéro d'appel interne pour la connexion et, éventuellement, les codes de prise d'appel.

8.7.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Applications**->**Adaptateur TFE**->**Adaptateur TFE**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Interface	Sélectionnez l'interface à laquelle connecter un adaptateur TFE. Toutes les interfaces FXS libres peuvent être sélectionnées.
Numéro d'appel interne	Sélectionnez le numéro d'appel interne configuré qui doit être affecté à l'adaptateur TFE. Le numéro d'appel est configuré dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**.
Code acceptation TFE	Lors de l'activation d'une touche de sonnerie au niveau de l'adaptateur TFE, un appel est déclenché dans le système. Pour établir une communication entre un abonné appelé et l'adaptateur TFE, cet abonné doit décrocher le combiné et

Champ	Description
	composer le code de prise d'appel. Saisissez ce code de prise d'appel. Si un abonné répond à un appel provenant d'un adaptateur TFE, le système de télécommunications compose automatiquement le code nécessaire pour établir la communication. L'abonné ne doit alors réaliser aucune autre saisie.

8.7.2 Signalisation TFE

Le menu **Applications**->**Adaptateur TFE**->**Signalisation TFE** permet de configurer les variantes de signalisation pour la prise d'appel via un adaptateur TFE. Il existe deux variantes d'appel TFE.

Le code de touche de sonnerie est le numéro d'appel composé par l'adaptateur TFE lors de l'activation de la touche de sonnerie dans le système. Cela vous permet de réaliser une répartition interne des appels pour chaque touche de sonnerie. Notez que les instructions de mise en marche de l'adaptateur TFE dépendent du fabricant. Reportez-vous au mode d'emploi fourni par le fabricant de l'adaptateur TFE.

8.7.2.1 Général

La zone **Général** vous permet de définir les caractéristiques principales de la signalisation TFE.

Le menu **Applications**->**Adaptateur TFE**->**Signalisation TFE**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Description	Sélectionnez l'un des dispositifs TFE configurés préalablement créés dans le menu **Applications**->**Adaptateur TFE**->**Adaptateur TFE**.
Code sonnerie	Saisissez un code à quatre chiffres clair pour la sonnerie. Lors de l'activation d'une touche de sonnerie au niveau de l'adaptateur TFE, les appareils terminaux entrés dans la variante d'appel TFE affectée sont appelés.
Nom de la sonnerie	Saisissez un nom pour la sonnerie.
Commuter la variante	Indiquez si les variantes d'appel TFE pour cette sonnerie

Champ	Description
	doivent être commutées via un calendrier configuré et, si tel est le cas, lequel. Pour chaque sonnerie, vous pouvez définir jusqu'à deux variantes d'appel TFE dans le menu **Applications**->**Adaptateur TFE**->**Signalisation TFE**->**Nouveau**->**Variante**. Valeurs possibles : • *Pas de calendrier, uniquement manuel* • *<Calendrier>*
Variante TFE active	Sélectionnez la variante d'appel TFE qui doit être activée par défaut pour cette sonnerie après la configuration.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Temps de signalisation des appels	Indiquez la durée en secondes pendant laquelle l'appel du portier doit être signalé. La valeur par défaut est *40* secondes.
Temps de franchissement	Saisissez ici le **Temps de franchissement** après lequel un transfert d'appel doit être effectué. La valeur par défaut est *15* secondes.
Appel en parallèle après le temps	Après un délai défini, il est possible d'appeler simultanément tous les numéros d'appel affectés à cette signalisation TFE. La valeur par défaut est *60* secondes.

8.7.2.2 Variante d'appel TFE 1 et 2

La zone **Variante d'appel TFE** permet de configurer les deux variantes d'appel TFE pour ce profil de signalisation.

Le menu **Applications**->**Adaptateur TFE**->**Signalisation TFE**->**Variante d'appel TFE** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Affectation	Indiquez où signaler une activation de la sonnette. Valeurs possibles : • *Interne* : la signalisation a lieu sur un numéro d'appel interne. • *Externe* : la signalisation a lieu sur un numéro d'appel externe.
Affectation interne	Sélectionnez les numéros d'appel internes sur lesquels une activation de la sonnette doit être signalée. Ajoutez un numéro d'appel interne à l'aide de l'option **Ajouter**.
Affectation externe	Indiquez le numéro de téléphone externe sur lequel une activation de la sonnette doit être signalée.
Signalisation	Vous pouvez appeler les numéros d'appel internes en utilisant l'appel général. Valeurs possibles : • *Simultané* (valeur par défaut) : tous les appareils terminaux attribués sont appelés simultanément. Si un téléphone est occupé, il est possible d'émettre un signal d'appel en attente. • *Linéaire* : tous les appareils terminaux attribués sont appelés de manière successive dans l'ordre indiqué dans la configuration. Si un appareil terminal est occupé, l'appareil terminal libre suivant est appelé. L'appel est signalé pendant env. 15 secondes à chaque abonné. Cette durée peut être réglée entre 1 et 99 secondes (pour chaque sonnerie). Si des abonnés téléphonent ou s'ils sont déconnectés, il n'y a aucun délai de transmission pour ces abonnés. • *En rotation* : cet appel est une exception à l'appel linéaire. Une fois que tous les appareils terminaux ont été appelés, la signalisation de l'appel recommence à partir du premier appareil terminal entré. L'appel est signalé jusqu'à ce que l'appelant raccroche ou jusqu'à ce que l'adaptateur TFE y mette fin (après env. deux minutes). • *Création* : les appareils terminaux sont appelés dans l'ordre indiqué dans la liste des abonnés de la configuration. Chaque appareil terminal déjà appelé est rappelé, jusqu'à ce

Champ	Description
	que tous les appareils terminaux entrés aient été appelés. La configuration vous permet de définir quand l'appareil terminal suivant doit être appelé. • *Linéaire, parallèle selon l'heure* : vous avez opté pour une configuration linéaire de l'appel TFE. Une fois la durée définie écoulée, vous pouvez indiquer dans la configuration que tous les abonnés de l'équipe doivent ensuite être appelés en parallèle (simultanément). • *En rotation, parallèle selon l'heure* : vous avez opté pour une configuration en rotation de l'appel TFE. Une fois la durée définie écoulée, vous pouvez indiquer dans la configuration que tous les abonnés TFE doivent ensuite être appelés en parallèle (simultanément).

8.8 Appels d'alarme

L'interface FXS des produits hybird peut être configurée comme entrée d'alarme. Un bouton d'alarme peut par exemple ainsi être relié à l'une de ces interfaces : lorsqu'une personne appuie sur le bouton, un appel d'alarme est déclenché et transmis soit à huit numéros d'appel internes maximum, soit à l'un des deux numéros d'appel externes. Pendant un appel d'alarme, l'un des contacts de commutation peut être activé, le cas échéant. La fonction peut éventuellement être commutée via un calendrier ou passer de l'une des variantes de signalisation possibles à l'autre.

8.8.1 Appels d'alarme

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour créer des entrées d'alarme.

8.8.1.1 Général

La zone **Général** vous permet de définir les caractéristiques principales des entrées d'alarme.

Le menu **Applications**->**Entrée d'alarme**->**Appels d'alarme**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
État	Activez ou désactivez la fonction. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Description	Saisissez une désignation claire pour l'appel d'alarme.
Interface	Sélectionnez l'interface devant être utilisée pour cet appel d'alarme.
Numéro d'appel interne	Sélectionnez un numéro d'appel interne devant être utilisé pour l'appel d'alarme.
Commuter la variante	Déterminez la manière dont l'appel d'alarme défini doit être activé. Valeurs possibles : • *Pas de calendrier, uniquement manuel* : la commutation manuelle est activée. • *<Entrée de calendrier>* : sélectionnez l'une des entrées de calendrier configurées pour l'appel d'alarme.
Variante d'appel active	Sélectionnez la variante d'appel qui doit être activée. Vous pouvez configurer les variantes après avoir confirmé la saisie sous l'onglet **Général** à l'aide du bouton **OK**.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Période de signalisation de l'alarme	Indiquez la durée en secondes pendant laquelle un appel d'alarme doit être signalé. La valeur par défaut est *30* secondes.
Répéter vers	Indiquez le temps en secondes entre les répétitions de l'appel d'alarme. Une valeur comprise entre *1* et *600* secondes est possible. La valeur par défaut est *10* secondes. Les répétitions d'appels d'alarme via une interface FXO sont

Champ	Description
	impossibles.
Nombre de répétitions	Indiquez le nombre de répétitions si un appel d'alarme n'est pas accepté. Une valeur comprise entre 1 et 10 répétitions est possible. La valeur par défaut est *2*. Les répétitions d'appels d'alarme via une interface FXO sont impossibles.
Horloger de connexion externe	Indiquez la durée maximale d'un appel d'alarme externe (en secondes) après l'acceptation de celui-ci. Une valeur comprise entre *1* et *600* secondes est possible. La valeur par défaut est *60* secondes.
Message d'information (UUS1)	Un message (max. 32 caractères) peut également être envoyé aux appareils terminaux RNIS.
Contact relais	Si un relais doit être commuté pendant l'appel d'alarme : sélectionnez le relais à utiliser. Le menu **Interfaces physiques**->**Relais** permet de configurer le relais.
Fichier wave	Indiquez si un fichier wave enregistré doit être lu lors de la prise de l'appel d'alarme, et sélectionnez le fichier en question, le cas échéant. Valeurs possibles : • *Arrêt* (valeur par défaut) : aucune musique d'attente ne doit être diffusée pour l'appelant mis en attente. • *<Fichier wave>* : l'abonné appelé doit entendre le fichier wave sélectionné.
Nombre d'émissions	Déterminez le nombre de fois consécutives que l'annonce doit être lue. Valeurs possibles : • *Sans fin (valeur par défaut)* • *1* à *10*

8.8.1.2 Variante 1 et 2

Vous pouvez configurer deux variantes de l'appel d'alarme. En général, l'une des variantes exploite la possibilité d'appeler des abonnés internes, et l'autre, celle d'appeler des abonnés externes.

Champs du menu Configuration de base

Champ	Description
Affectation	Vous pouvez affecter les appels d'alarme soit à huit numéros d'appel internes maximum, soit à deux numéros d'appel externes. Indiquez si les appels d'alarme doivent être signalés aux abonnés internes ou externes. Valeurs possibles : • *Externe* : le numéro d'appel externe entré est appelé. En cas d'appel d'alarme, deux numéros d'appel externes peuvent être appelés en alternance. • *Interne* (valeur par défaut) : les abonnés affectés aux numéros d'appel sélectionnés sont appelés selon la signalisation configurée. En cas d'appel d'alarme, huit abonnés internes peuvent être appelés simultanément.
Premier numéro d'appel externe	Uniquement pour **Affectation** = *Externe* Saisissez le premier numéro d'appel de l'abonné externe.
Deuxième numéro d'appel externe	Uniquement pour **Affectation** = *Externe* Saisissez le deuxième numéro d'appel de l'abonné externe.
Affectation interne	Uniquement pour **Affectation** = *Interne* Sélectionnez les abonnés internes. Ajoutez des numéros d'appel internes à l'aide de l'option **Ajouter**.

8.9 Système boîte vocale

Le système boîte vocale est un répondeur intelligent pour les utilisateurs de votre appareil **hybird**. Une boîte vocale individuelle peut être configurée pour chaque poste secondaire. Grâce à un code PIN personnel, tous les abonnés peuvent écouter, enregistrer ou supprimer leurs messages depuis n'importe quel téléphone.

Les abonnés peuvent être informés par e-mail des appels entrants. Les messages enre-

gistrés peuvent être transférés automatiquement à une adresse e-mail de votre choix.

Les paramètres généraux du système boîte vocale sont appliqués sur votre appareil **hybird**. L'utilisation de la boîte vocale individuelle s'effectue via un téléphone.

Chaque abonné peut utiliser sa boîte vocale individuelle en déviant son téléphone vers sa boîte vocale.

Note

Si vous souhaitez utiliser une boîte vocale, vous avez besoin d'une carte SD. Le cas échéant, vous devez charger la structure de dossier nécessaire avec les textes d'annonce sur la carte SD. Dans le menu **Maintenance**->**Logiciel et configuration**, sélectionnez pour ce faire l'option *Importer les fichiers Voice Mail Wave*.

Attention

N'enlevez pas la carte SD pendant une opération de lecture ou d'écriture afin d'éviter de perdre des données ou d'endommager la carte. Observez la LED correspondante dans la partie supérieure de l'appareil : elle clignote lors d'une opération de lecture ou d'écriture.

8.9.1 Boîtes vocales

Le menu **Applications**->**Système boîte vocale**->**Boîtes vocales** affiche une liste des boîtes vocales individuelles des différents abonnés, pour autant que des boîtes vocales soient configurées.

Valeurs de la liste Boîtes vocales

Champ	Description
Numéro d'appel interne	Permet d'afficher le numéro d'appel de l'abonné interne pour lequel la boîte vocale est configurée.
Utilisateur	Permet d'afficher le nom de l'abonné interne pour lequel la boîte vocale est configurée.
Langue	Permet d'afficher la langue des textes d'annonce de la boîte vocale. L'option *Par défaut* signifie que la langue définie

Champ	Description
	dans le menu **Applications**->**Système boîte vocale**->**Général** pour l'ensemble du système boîte vocale est utilisée.
Notification	Permet d'indiquer si l'abonné est informé des appels manqués.
Variante d'appel active	Permet d'afficher l'état de la boîte vocale (*Au bureau* ou *En extérieur*).
Affectation de licence	Permet d'indiquer si une licence est actuellement affectée à une boîte vocale. **Note** Le nombre de boîtes vocales configurées ne peut pas dépasser le nombre de licences disponibles. Vous devez toutefois veiller à ce que le nombre de boîtes vocales utilisées corresponde au nombre de licences.

8.9.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour ajouter des entrées.

Le menu **Applications**->**Système boîte vocale**->**Boîtes vocales**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Numéro d'appel interne	Sélectionnez le numéro d'appel interne de l'abonné pour lequel vous souhaitez configurer une boîte vocale. Vous pouvez choisir parmi les numéros d'appel internes qui sont configurés dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**.
Langue Boîte vocale	Sélectionnez la langue souhaitée pour les annonces de la boîte vocale. Valeurs possibles : • *Deutsch* : la boîte vocale utilise des textes en allemand.

Champ	Description
	• *Néerlandais* : la boîte vocale utilise des textes en néerlandais. • *Englisch* : la boîte vocale utilise des textes en anglais. • *Italien* : la boîte vocale utilise des textes en italien. • *Français* : la boîte vocale utilise des textes en français. • *Par défaut* (valeur par défaut) : la boîte vocale utilise la langue définie dans le menu **Applications**->**Boîte vocale**->**Général** pour l'ensemble du système boîte vocale. **Note** Vous devez opter pour un paramètre autre que *Par défaut* uniquement si, au sein de votre système boîte vocale, vous souhaitez utiliser différentes langues pour les boîtes vocales.
Adresse e-mail (provenant des paramètres utilisateur)	Ce champ indique l'adresse e-mail de l'utilisateur à laquelle une notification doit être envoyée lorsqu'un message est laissé sur la boîte vocale. L'adresse e-mail est enregistrée dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Configuration de base**.
Notification par e-mail	Si une personne a laissé un message sur la boîte vocale, une notification peut être envoyée à l'abonné. Valeurs possibles : • *aucun* (valeur par défaut) : L'abonné ne reçoit pas de notification. • *E-mail* : l'abonné est informé par e-mail lorsqu'une personne lui a laissé un message. • *E-mail avec annexe* : si un appelant a laissé un message, l'abonné reçoit un e-mail avec en pièce jointe l'enregistrement du message. • *Personnalisé* : lorsque l'administrateur libère la fonction *Personnalisé*, la configuration de la notification par e-mail peut être modifiée par l'utilisateur sous **Accès utilisateur**. Si l'administrateur définit une autre valeur, l'utilisateur ne peut effectuer aucune modification.

Champ	Description
	Note Après qu'un abonné a été informé de la présence d'un message par e-mail, l'**État** de la communication change en fonction des paramètres définis dans le menu **Accès utilisateur**. Dans le menu **Accès utilisateur**->**Système boîte vocale**->**Paramètres**, sous **Comportement du transfert d'e-mail**, vous pouvez configurer le comportement de l'état.
Durée d'enregistrement maxi	Indiquez la durée maximale d'enregistrement par message. Les valeurs possibles sont comprises entre *5* et *300* secondes, la valeur par défaut est *180* secondes.
Calendrier pour état "en extérieur"	Lorsque l'abonné n'est pas là, la boîte vocale peut être commutée via un calendrier. Si un calendrier doit être utilisé, celui-ci doit être configuré dans le menu **Applications**->**Calendrier** avec le paramètre **Application** = *Système boîte vocale*. Valeurs possibles : • *Pas de calendrier, uniquement manuel* (valeur par défaut) : l'abonné peut activer ou désactiver manuellement la boîte vocale. • <Calendrier> : la boîte vocale peut être activée ou désactivée aux moments définis dans le calendrier sélectionné.

Champs du menu Paramètres de l'utilisateur

Champ	Description
État du propriétaire de la boîte mail	Définissez le mode de fonctionnement de la boîte vocale lors du démarrage du système boîte vocale. Valeurs possibles : • *Au bureau* (valeur par défaut) : sélectionnez ce paramètre si l'abonné se trouve au bureau lors du démarrage du système boîte vocale. • *En extérieur* : sélectionnez ce paramètre si l'abonné est

Champ	Description
	absent lors du démarrage du système boîte vocale.
Vérifier PIN	Indiquez si la boîte vocale actuellement configurée doit être protégée par un PIN. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Vous pouvez modifier le PIN de la boîte vocale personnelle dans le menu **Numérotation**->**Paramètres de l'utilisateur**->**Utilisateur**->**Autorisations**, sous **PIN pour accès par téléphone**.
Mode pour état "Au bureau"	La boîte vocale peut fonctionner selon deux modes de configuration pendant les heures de bureau. Valeurs possibles : • *Annonce et enregistrement* (valeur par défaut) : un appelant entend une annonce et peut laisser un message. • *Uniquement annonce* : un appelant entend une annonce, mais ne peut pas laisser de message lui-même.
Calendrier pour état "en extérieur"	La boîte vocale peut fonctionner selon deux modes de configuration en dehors des heures de bureau. Valeurs possibles : • *Uniquement annonce* (valeur par défaut) : un appelant entend une annonce, mais ne peut pas laisser de message lui-même. • *Annonce et enregistrement* : un appelant entend une annonce et peut laisser un message.

8.9.2 État

Le menu **Applications**->**Boîte vocale**->**État** indique l'état des boîtes vocales individuelles des différents abonnés. Vous pouvez voir le nombre de nouveaux appels arrivés sur quelle boîte vocale, ainsi que le nombre d'anciens appels existants.

Valeurs de la liste Messages système

Champ	Description
Numéro d'appel interne	Permet d'afficher le numéro d'appel de l'abonné interne pour lequel la boîte vocale est configurée.
Utilisateur	Permet d'afficher le nom de l'abonné interne pour lequel la boîte vocale est configurée.
Nouveaux appels	Permet d'afficher les appels qui n'ont pas encore été écoutés par l'abonné.
Anciens appels	Permet d'afficher les appels déjà écoutés ou enregistrés par l'abonné.

8.9.3 Général

Ce menu vous permet de configurer les paramètres généraux pour votre système boîte vocale.

Le menu **Applications**->**Boîte vocale**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Système boîte vocale	Indiquez si votre système boîte vocale doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Description	Activé uniquement pour **Système boîte vocale**. Saisissez une description pour votre système boîte vocale. Si un téléphone arrive sur le système boîte vocale, cette description est affichée sur le téléphone. La valeur par défaut est *Boîte vocale*.
Numéro d'appel interne	Activé uniquement pour **Système boîte vocale**. Saisissez le numéro d'appel interne auquel votre système boîte vocale est joignable. La valeur par défaut est *50*.

Champ	Description
Langue	Sélectionnez la langue pour l'ensemble du système boîte vocale. Valeurs possibles : • *Deutsch* (valeur par défaut) • *Néerlandais* • *Englisch* • *Italien* • *Français* En fonction de la langue configurée ici, il est possible de définir une langue individuellement pour chaque boîte vocale, dans le menu **Applications**->**Boîte vocale**->**Boîtes vocales**->**Nouveau**.

Champs du menu Paramètres mail

Champ	Description
Serveur SMTP	Saisissez l'adresse (adresse IP ou nom DNS valide) du serveur de messagerie qui doit être utilisé pour l'envoi d'e-mails.
Port serveur SMTP	Saisissez le port qui doit être utilisé pour l'envoi d'e-mails. La valeur par défaut est *25*.
Adresse de l'expéditeur	Saisissez une adresse qui doit être utilisée comme expéditeur lors de l'envoi d'e-mails. L'adresse sert uniquement à identifier les e-mails dans la boîte de réception.
Nom de l'utilisateur SMTP	Saisissez le nom d'utilisateur pour le serveur SMTP.
Mot de passe SMTP	Saisissez le mot de passe pour l'utilisateur du serveur SNMP.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Durée de vie	Les messages vocaux sont automatiquement effacés après une durée configurable.

Champ	Description
	Les valeurs possibles sont comprises entre *10* et *60* jours. La valeur par défaut est *60*.

Chapitre 9 LAN

Ce menu vous permet de configurer les adresses de votre LAN et de structurer votre réseau local par des VLAN.

9.1 Configuration IP

Ce menu sert également à éditer la configuration IP du LAN et les interfaces Ethernet de votre appareil.

9.1.1 Interfaces

Le menu **LAN**->**Configuration IP**->**Interfaces** contient la liste des interfaces IP disponibles. Vous pouvez modifier la configuration IP des interfaces ou créer des interfaces virtuelles pour des applications spéciales. Vous trouverez ici une liste de toutes les interfaces configurées dans le menu **Gestion du système**->**Mode Interface / groupes Bridge**->**Interfaces** (interfaces Ethernet logiques et celles créées dans les sous-systèmes).

Le symbole permet d'éditer les paramètres d'une interface existante (groupes de ponts, interfaces Ethernet en mode routage).

Le bouton **Nouveau** sert à créer des interfaces virtuelles. Ceci n'est toutefois nécessaire que pour les applications spéciales (BRRP, etc.).

En fonction de l'option sélectionnée, différents champs et options sont disponibles. Vous trouverez ci-dessous une liste de toutes les possibilités de configuration.

Note

Remarque :

Si lors de la première configuration, votre appareil a obtenu dynamiquement une adresse IP par un serveur DHCP exploité dans votre réseau, l'adresse IP standard est effacée automatiquement et votre appareil n'est alors plus joignable via cette ancienne adresse.

Si lors de la première configuration, vous avez établi la connexion avec l'appareil via l'adresse IP standard ou avez attribué une adresse IP avec le **Dime Manager**, votre appareil sera accessible via cette adresse. il ne peut plus obtenir de configuration IP dynamique par DHCP.

Exemple réseaux partiels

Si votre appareil est connecté à un LAN composé de deux réseaux partiels, vous devez saisir pour le second réseau partiel une seconde **Adresse IP/Masque de réseau**.

Le premier réseau partiel possède par ex. deux hôtes avec les adresses IP 192.168.42.1 et 192.168.42.2, et dans le second réseau partiel deux hôtes avec les adresses IP 192.168.46.1 et 192.168.46.2. Afin de pouvoir échanger des paquets de données avec le premier réseau partiel, votre appareil utilise par ex. l'adresse IP 192.168.42.3 et pour le second réseau partiel l'adresse IP 192.168.46.3. Les masques de réseau pour les deux réseaux partiels doivent être indiqués également.

9.1.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour créer des interfaces virtuelles.

Le menu **LAN**->**Configuration IP**->**Interfaces**-> **/Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Sur la base de l'interface Ethernet	Ce champ ne s'affiche que si une interface de routage virtuelle est éditée. Choisissez l'interface Ethernet pour laquelle l'interface virtuelle doit être configurée.
Mode adresses	Choisissez comment affecter une adresse IP à l'interface. Valeurs possibles : • *Statique* (valeur par défaut) : Une adresse IP statique dans **Adresse IP/Masque de réseau** est affectée à l'interface. • *DHCP* : l'interface reçoit une adresse IP de manière dynamique avec DHCP.
Adresse IP/Masque de réseau	Uniquement pour **Mode adresses** = *Statique* Ajoutez une nouvelle entrée d'adresse par **Ajouter** et indiquez l'**Adresse IP** ainsi que le **Masque réseau** correspondant de l'interface virtuelle.

Champ	Description
Mode interfaces	Uniquement pour les interfaces physiques en mode routage. Sélectionnez le mode de configuration de l'interface. Valeurs possibles : • *Untagged* (valeur par défaut) : L'interface n'est affectée à aucune utilisation spécifique. • *Tagged (VLAN)*: Cette option ne s'applique qu'aux interfaces de routage. Cette option permet d'affecter l'interface à un réseau VLAN. Cela est réalisé à l'aide de l'identifiant VLAN qui s'affiche dans ce mode et peut alors être configuré. La définition d'une adresse MAC dans **Adresse MAC** est optionnelle dans ce mode.
Adresse MAC	Uniquement pour les interfaces virtuelles et pour le **Mode interfaces** = *Untagged* Saisissez l'adresse MAC liée à l'interface. Vous pouvez utiliser pour les interfaces virtuelles l'adresse MAC de l'interface physique sous laquelle l'interface virtuelle a été créée. Toutefois, cela n'est pas obligatoire. L'affectation d'une adresse MAC virtuelle est également possible. Les 6 premiers caractères de l'adresse MAC sont prédéfinis (bien qu'ils puissent être modifiés).
ID VLAN	Uniquement pour **Mode interfaces** = *Tagged (VLAN)* Cette option ne s'applique qu'aux interfaces de routage. Affectez l'interface à un réseau VLAN en saisissant l'identifiant VLAN du VLAN correspondant. Les valeurs possibles sont comprises entre *1* (valeur par défaut) et *4094*.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Adresse MAC DHCP	Uniquement pour **Mode adresses** = *DHCP*

Champ	Description
	Si **Utiliser prédéfini** est activé (réglage par défaut), l'adresse MAC matérielle de l'interface Ethernet est utilisée. Pour les interfaces physiques, l'adresse MAC actuelle est complétée par défaut. Si vous désactivez l'option **Utiliser prédéfini**, vous devez saisir une adresse MAC pour l'interface virtuelle, par ex. *00:e1:f9:06:bf:03*. Certains fournisseurs d'accès utilisent des adresses MAC indépendantes du matériel pour affecter les adresses IP de manière dynamique à leurs clients. Si votre fournisseur d'accès vous a attribué une adresse MAC, vous devez la saisir ici.
Nom d'hôte DHCP	Uniquement pour **Mode adresses** = *DHCP* Indiquez le nom d'hôte qui est exigé par le fournisseur d'accès. L'entrée doit contenir 45 caractères maximum.
DHCP Broadcast Flag	Uniquement pour **Mode adresses** = *DHCP* Choisissez si le bit BROADCASTS doit être activé ou non dans les demandes DHCP de votre appareil. Certains serveurs DHCP attribuant les adresses IP par UNICAST ne réagissent pas aux demandes DHCP avec bit BROADCAST activé. Dans ce cas, vous devez envoyer des demandes DHCP dans lesquelles ce bit n'est pas activé. Si tel est le cas, désactivez cette option. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Proxy ARP	Choisissez ci votre appareil doit répondre aux demandes ARP de son propre réseau LAN à la place de dispositifs définis. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
TCP-MSS-Clamping	Choisissez si votre appareil doit appliquer le procédé « MSS Clamping ». Pour empêcher la fragmentation des paquets IP, l'appareil diminue alors automatiquement la MSS (Maximum Segment Size) à la valeur indiquée ici.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Si l'option est activée, la valeur par défaut *1350* est inscrite dans le champ de saisie.

9.2 VLAN

Grâce à l'implémentation de la segmentation VLAN selon 802.1Q, la configuration de réseaux VLAN est possible depuis votre appareil. Notamment les ports sans fil d'un point d'accès sont en mesure de supprimer le Tag VLAN d'un bloc de transmission de données envoyé aux clients et d'étiqueter les blocs de transmission de données reçus avec un identifiant VLAN défini préalablement. Grâce à cette fonctionnalité, un point d'accès n'est rien d'autre qu'un switch compatible avec VLAN avec l'extension de rassembler les clients en groupes de VLAN. De manière générale, la segmentation VLAN est configurable depuis toutes les interfaces.

VLAN pour pontage et VLAN pour routage

Le menu **LAN**->**VLAN** permet de configurer les réseaux VLAN (réseaux vLAN virtuels) avec des interfaces fonctionnant en mode pontage. Le menu **VLAN** vous permet de procéder à tous les réglages nécessaires à cet effet et d'interroger leur état.

Attention

Pour les interfaces fonctionnant en mode routage, l'interface respective se voit simplement affecter un identifiant VLAN. Vous pouvez le définir à l'aide des paramètres **Mode interfaces** = *Tagged (VLAN)* et le champ **ID VLAN** dans le menu **LAN**->**Configuration IP**->**Interfaces**->**Nouveau**.

9.2.1 VLAN

Ce menu vous permet d'afficher tous les réseaux VLAN déjà configurés, de modifier vos réglages et de créer de nouveaux réseaux VLAN. Par défaut, vous disposez de la *gestion* VLAN à laquelle toutes les interfaces sont affectées.

9.2.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres réseaux VLAN supplémentaires.

Le menu **LAN**->**VLAN**->**VLAN**->**Nouveau** se compose des champs suivants :

Champs du menu Configurer VLAN

Champ	Description
Identifiant VLAN	Saisissez le chiffre identifiant le réseau VLAN. Le menu ne permet plus de modifier cette valeur. Les valeurs possibles sont comprises entre *1* et *4094*
Nom VLAN	Saisissez un nom univoque pour le réseau VLAN. Une chaîne peut contenir 32 caractères maximum.
Membres VLAN	Sélectionnez les ports devant appartenir à ce réseau VLAN. Le bouton **Ajouter** vous permet d'ajouter des membres supplémentaires. Pour chaque entrée, continuez à définir si les blocs de transmission de données transmis par ce port doivent être transmis *Tagged* (c'est-à-dire avec des informations VLAN) ou *Untagged* (c'est-à-dire sans informations VLAN).

9.2.2 Configuration du port

Ce menu vous permet de définir et de visualiser les règles pour la réception de blocs de transmission de données aux ports du VLAN.

Le menu **LAN**->**VLAN**->**Configuration du port** se compose des champs suivants :

Champs du menu Configuration du port

Champ	Description
Interface	Indique le port pour lequel vous définissez le PVID et les règles de traitement.
PVID	Affectez au port sélectionné le PVID (Port VLAN Identifier) souhaité.

Champ	Description
	Si un paquet sans étiquette VLAN atteint ce port, il est doté de ce PVID.
Rejeter les frames sans balise	Si l'option est activée, les blocs de transmission de données sans étiquettes sont rejetés. Si l'option est désactivée, les blocs de transmission de données sans étiquettes sont dotés du PVID défini dans le présent menu.
Rejeter les non-membres	Si l'option est activée, tous les blocs de transmission de données étiquetés sont rejetés si l'identifiant VLAN de leur étiquette ne correspond pas au groupe du port sélectionné.

9.2.3 Administration

Ce menu vous permet de procéder à la configuration de base pour un réseau VLAN. Les options doivent être configurées séparément pour chaque groupe de pont.

Le menu **LAN**->**VLAN**->**Administration** se compose des champs suivants :

Champs dans le menu groupe de pont br<ID> Options VLAN

Champ	Description
Activer VLAN	Activez ou désactivez le groupe de pont spécifique pour le réseau VLAN. Sélectionnez `Activé` pour activer la fonction. La fonction est désactivée par défaut.
VID de gestion	Choisissez l'identifiant VLAN du réseau VLAN dans lequel votre appareil doit fonctionner.

Chapitre 10 Réseau

10.1 Routes

Route par défaut (Default Route)

En cas de route par défaut, toutes les données sont automatiquement transmises vers une connexion, si aucune autre route adaptée n'est disponible. Lorsque vous établissez un accès à Internet, vous entrez la route vers votre FAI (fournisseur d'accès à Internet) comme route par défaut. Si vous créez par exemple un connexion à un réseau d'entreprise, vous n'entrez la route vers le siège ou la filiale comme route par défaut que si vous n'établissez pas d'accès à Internet depuis votre appareil. Si par exemple vous établissez à la fois un accès à Internet et une connexion à un réseau d'entreprise, vous entrez une route par défaut vers le FAI et une route de réseau vers le siège. Vous pouvez entrer sur votre appareil plusieurs routes par défaut, mais une seule peut être active à un moment donné. Veillez donc aux différentes valeurs pour la **Métrique**, si vous entrez plusieurs routes par défaut.

10.1.1 Configuration des routes IPv4

Le menu **Réseau**->**Routes**->**Configuration des routes IPv4** propose une liste de toutes les routes configurées.

10.1.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour créer d'autres routes.

Lorsque l'option *Etendu* est sélectionnée pour la **Classe de routes**, une nouvelle section de configuration apparaît.

Le menu **Réseau**->**Routes**->**Configuration des routes IPv4**->**Nouveau** se compose des champs suivants :

Champ du menu Paramètres de base

Champ	Description
Type de routes	Sélectionnez le type de route.

Champ	Description
	Valeurs possibles : • *Route par défaut via une interface* : route via une interface spécifique utilisée si aucune autre route adaptée n'est disponible. • *Route par défaut via une passerelle* : route via une passerelle spécifique utilisée si aucune autre route adaptée n'est disponible. • *Route hôte via interface* : route vers un hôte unique via une interface spécifique. • *Route hôte via passerelle* : route vers un hôte unique via une passerelle spécifique. • *Route de réseau via l'interface* (valeur par défaut) : route vers un hôte via une interface spécifique. • *Route de réseau via la passerelle* : route vers un hôte via une passerelle spécifique. Uniquement pour les interfaces utilisées en mode client DHCP : même si une interface est configurée pour le mode client DHCP, il est possible de configurer des routes pour l'échange de données via cette interface. Les paramètres obtenus par le serveur DHCP sont alors repris dans le tableau de routage actif avec les paramètres configurés ici. Cela permet par exemple, avec des adresses de passerelles dynamiques, de conserver certaines routes ou de définir des routes avec une mesure différente (une priorité différente). Par contre, si le serveur DHCP transmet des routes statiques (Classless Static Routes), les paramètres configurés ici ne sont pas repris dans le routage. • *Modèle pour route par défaut avec DHCP* : les informations de routage sont entièrement reprises par le serveur DHCP. Seuls les paramètres étendus peuvent également être configurés. Cette route n'est pas modifiée par les autres routes définies pour cette interface. Elle est reprise parallèlement à celles-ci dans le tableau de routage. • *Modèle pour route hôte avec DHCP* : les paramètres reçus via DHCP sont complétées avec des informations de routage sur un hôte donné.

Champ	Description
	• *Modèle pour route de réseau avec DHCP* : les paramètres reçus via DHCP sont complétées avec des informations de routage sur un réseau donné. **Note** Lorsque le bail DHCP échoit ou lors d'un redémarrage de l'appareil, les routes issues de l'association des paramètres DHCP et des réglages réalisés ici sont de nouveau effacées du routage actif. Elles sont de nouveau générées et activées en présence d'une nouvelle configuration DHCP.
Interface	Sélectionnez l'interface devant être utilisée pour cette route.
Classe de routes	Sélectionnez le type de **Classe de routes**. Valeurs possibles : • *Par défaut* : définit une route avec les paramètres standard. • *Etendu* : définissez si la route doit être définie avec des paramètres étendus. Si cette fonction est active, une route est définie avec des paramètres de routage étendus, comme interface source et adresse IP source, ainsi que protocole, port source et cible, type du service et statut de l'interface des appareils.

Champs du menu Paramètres de routage

Champ	Description
Adresse IP locale	Uniquement pour **Type de routes** = *Route par défaut via une interface*, *Route hôte via interface* ou *Route de réseau via l'interface* Entrez l'adresse IP de l'hôte auquel votre appareil doit transmettre le paquet IP.
Adresse IP de destination/Masque de réseau	Uniquement pour **Type de routes** *Route hôte via interface* ou *Route de réseau via l'interface*

Champ	Description
	Saisissez l'adresse IP de l'hôte cible ou du réseau cible. Si **Type de routes** = *Route de réseau via l'interface* Indiquez également dans le deuxième champ le masque de réseau correspondant.
Adresse IP de la passerelle	Uniquement pour **Type de routes** = *Route par défaut via une passerelle*, *Route hôte via passerelle* ou *Route de réseau via la passerelle* Entrez l'adresse IP de la passerelle auquel votre appareil doit transmettre le paquet IP.
Métrique	Sélectionnez la priorité de la route. Plus la valeur que vous définissez est basse, plus la priorité de la route est élevée. Plage de valeurs de *0* à *15*. La valeur par défaut est *1*.

Champs du menu Paramètres de route étendus

Champ	Description
Description	Saisissez une description pour la route IP.
Interface source	Sélectionnez l'interface devant être utilisée pour transmettre le paquet de données à l'appareil. La valeur par défaut est *aucun*.
Adresse IP source/ Masque de réseau	Saisissez l'adresse IP et le masque de réseau de l'hôte source ou du réseau source.
Protocole couche 4	Sélectionnez un protocole. Valeurs possibles : *ICMP*, *IGMP*, *TCP*, *UDP*, *GRE*, *ESP*, *AH*, *OSPF*, *PIM*, *L2TP*, *Quelconque*. La valeur par défaut est *Quelconque*.
Port source	Uniquement pour **Protocole couche 4** = *TCP* ou *UDP* Saisissez le port source.

Champ	Description
	Sélectionnez d'abord la plage de numéros de ports. Valeurs possibles : • *Quelconque* (valeur par défaut) : La route est valable pour tous les numéros de ports. • *Unique* : permet la saisie d'un numéro de port. • *Plage* : permet la saisie d'une plage de numéros de ports. • *Privilégié* : saisie de numéros de ports privilégiés : 0 ... 1023. • *Serveur* : saisie de numéros de ports de serveurs : 5000 ... 32767. • *Clients 1* : saisie de numéros de ports clients : 1024 ... 4999. • *Clients 2* : saisie de numéros de ports clients : 32768 ... 65535. • *Non privilégié* : saisie de numéros de ports non privilégiés : 1024 ... 65535. En fonction de la sélection de la plage de numéros de ports, saisissez les valeurs correspondantes sous **Port** (port seul ou port de démarrage) et, le cas échéant, sous **jusqu'à port** (port de fin).
Port de destination	Uniquement pour **Protocole couche 4** = *TCP* ou *UDP* Saisissez le port cible. Sélectionnez d'abord la plage de numéros de ports. Valeurs possibles : • *Quelconque* (valeur par défaut) : La route est valable pour tous les numéros de ports. • *Unique* : permet la saisie d'un numéro de port. • *Plage* : permet la saisie d'une plage de numéros de ports. • *Privilégié* : saisie de numéros de ports privilégiés : 0 ... 1023. • *Serveur* : saisie de numéros de ports de serveurs : 5000 ... 32767. • *Clients 1* : saisie de numéros de ports clients : 1024 ...

Champ	Description
	4999. • *Clients 2* : saisie de numéros de ports clients : 32768 ... 65535. • *Non privilégié* : saisie de numéros de ports non privilégiés : 1024 ... 65535. En fonction de la sélection de la plage de numéros de ports, saisissez les valeurs correspondantes sous **Port** (port seul ou port de démarrage) et, le cas échéant, sous **jusqu'à port** (port de fin).
Valeur DSCP/TOS	Sélectionnez le type de service (TOS, Type of Service). Valeurs possibles : • *Ignorer* (valeur par défaut) : Le type de service n'est pas pris en compte. • *Valeur binaire DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire). • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au format binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63. • *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F. Indiquez la valeur appropriée pour *Valeur binaire DSCP*, *Valeur décimale DSCP*, *Valeur hexadécimale DSCP*, *Valeur binaire TOS*, *Valeur décimale TOS* et *Valeur hexadécimale TOS*.
Mode	Indiquez quand l'interface définie dans **Paramètres de routage**->**Interface** doit être utilisée.

Champ	Description
	Valeurs possibles : • *Composer et attendre* (valeur par défaut) : la route peut être utilisée lorsque l'interface est « active ». Si l'interface est « en veille », sélectionnez-la et attendez qu'elle soit « active ». • *Obligatoire* : la route est toujours utilisable. • *Composer et continuer* : la route peut être utilisée lorsque l'interface est « active ». Si l'interface est « en veille », sélectionnez-la et utilisez la route alternative jusqu'à ce que l'interface soit « active ». • *Ne jamais sélectionner* : la route peut être utilisée lorsque l'interface est « active ». • *Toujours composer* : la route peut être utilisée lorsque l'interface est « active ». Si l'interface est « en veille », sélectionnez-la et attendez qu'elle soit « active ». Le routage est alors réalisé avec une interface alternative avec une moins bonne métrique, jusqu'à ce que l'interface soit « active ».

10.1.2 Tableau de routage IPv4

Le menu **Réseau**->**Routes**->**Tableau de routage IPv4** propose une liste de toutes les routes IPv4. Les routes ne doivent pas toutes être actives, mais peuvent à tout moment être activées avec un échange de données approprié.

Champs du menu Tableau de routage IPv4

Champ	Description
Adresse IP de destination	Indique l'adresse IP de l'hôte cible ou du réseau cible.
Masque réseau	Indique le masque de réseau de l'hôte cible ou du réseau cible.
Passerelle	Indique l'adresse IP de la passerelle. Rien n'apparaît ici dans le cas de routes reçues via DHCP.
Interface	Indique l'interface utilisée pour cette route.
Métrique	Indique la priorité de la route. Plus la valeur est basse, plus la priorité de la route est élevée.
Type de routes	Indique le type de route.

Champ	Description
Route étendue	Indique si une route a été configurée avec des paramètres étendus.
Supprimer	Le symbole vous permet de supprimer des entrées.

10.1.3 Options

Contrôle de la route de retour

Le terme « Contrôle de la route de retour » (« Back Route Verify » en anglais) désigne une fonction simple mais très puissante. Lorsque le contrôle est activé sur une interface, elle n'accepte des paquets de données entrants que si des paquets de réponse sortants sont routés depuis la même interface. Vous pouvez ainsi éviter (même sans filtre) l'acceptation de paquets avec des adresses IP falsifiées.

Le menu **Réseau**->**Routes**->**Options** se compose des champs suivants :

Champs du menu Vérification de la route de retour

Champ	Description
Mode	Sélectionnez ici comment spécifier les interfaces pour lesquelles un contrôle de la route de retour est activée. Valeurs possibles : • *Activer pour toutes les interfaces* : le contrôle de la route de retour est activé pour toutes les interfaces. • *Activer pour certaines interfaces* (valeur par défaut) : Une liste des interfaces dans lesquelles le contrôle de la route de retour n'est activé que pour certaines interfaces est affichée. • *Désactiver pour toutes les interfaces* : le contrôle de la route de retour est désactivé pour toutes les interfaces.
N°	Uniquement pour **Mode** = *Activer pour certaines interfaces* Indique le numéro d'ordre de l'entrée de la liste.
Interface	Uniquement pour **Mode** = *Activer pour certaines interfaces*

Champ	Description
	Permet d'afficher le nom de l'interface.
Vérification de la route de retour	Uniquement pour **Mode** = *Activer pour certaines interfaces* Indiquez si *Vérification de la route de retour* doit être activé pour cette interface. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut pour toutes les interfaces.

10.2 NAT

Network Address Translation (NAT) est une fonction de votre appareil permettant de convertir les adresses source et cible des paquets IP de manière définie. Lorsque NAT est activé, les connexions IP ne sont plus autorisées par défaut que dans un sens, sortantes (forward) (= fonction de protection). Des règles d'exception peuvent être configurées (dans *Configuration NAT* sur la page 212).

10.2.1 Interfaces NAT

Le menu **Réseau**->**NAT**->**Interfaces NAT** présente une liste de toutes les interfaces NAT.

Les options *NAT actif*, *Loopback actif*, *Rejet sans notification* et *PPTP-Passthrough* peuvent être sélectionnées pour chaque interface NAT.

Transfert de port indique par ailleurs combien de règles de transmission de port ont été configurées pour cette interface.

Options dans le menu Interfaces NAT

Champ	Description
NAT actif	Indiquez si NAT doit être activé pour l'interface. La fonction est désactivée par défaut.
Loopback actif	La fonction Loopback NAT permet l'utilisation de NAT même avec des connexions sur lesquelles NAT n'est pas activé. Elle est utilisée pour interpréter des demandes sur le LAN comme

Champ	Description
	si elles provenaient du WAN. Vous pouvez tester ainsi les Server Services. La fonction est désactivée par défaut.
Rejet sans notification	Indiquez si les paquets IP doivent être refusés tacitement par NAT. Si cette fonction est désactivée, l'émetteur des paquets IP refusés en est informé par un message RST ICMP ou TCP correspondant. La fonction est désactivée par défaut.
PPTP-Passthrough	Indiquez si l'établissement et l'utilisation simultanées de plusieurs connexions PPTP sortantes par les hôtes du réseau doivent être autorisés même lorsque NAT est activé. La fonction est désactivée par défaut. Si **PPTP-Passthrough** est activé, votre appareil ne doit pas être configuré comme point d'extrémité de tunnel.
Transfert de port	Indique le nombre de règles de transmission port configurées dans **Réseau**->**NAT**->**Configuration NAT**.

10.2.2 Configuration NAT

Le menu **Réseau**->**NAT**->**Configuration NAT** permet d'extraire facilement des données du NAT, en plus de convertir des adresses et des ports. Vous pouvez configurer différentes méthodes NAT pour l'échange de données sortantes : vous pouvez définir comment un hôte externe peut établir une connexion avec un hôte interne.

10.2.2.1 Nouveau

Sélectionnez le bouton **Nouveau** pour créer configurer NAT.

Le menu **Réseau**->**NAT**->**Configuration NAT**->**Nouveau** se compose des champs suivants :

Champ du menu Paramètres de base

Champ	Description
Description	Saisissez une description pour la configuration NAT.

Champ	Description
Interface	Sélectionnez l'interface pour laquelle NAT doit être configuré. Valeurs possibles : • *Quelconque* (valeur par défaut) : Le NAT est configuré pour toutes les interfaces. • *<Nom de l'interface>* : Sélectionnez l'une des interfaces dans la liste.
Type d'échange de données	Sélectionnez le type d'échange de données pour lequel NAT doit être configuré. Valeurs possibles : • *entrant (NAT de destination)* (valeur par défaut) : l'échange de données provenant de l'extérieur. • *sortant (NAT source)* : l'échange de données partant vers l'extérieur. • *exclusif (sans NAT)* : l'échange de données depuis NAT.
Méthode NAT	Uniquement pour **Type d'échange de données** = *sortant (NAT source)* Sélectionnez la méthode NAT pour l'échange de données sortantes. Le point de départ pour la sélection de la méthode NAT est un scénario NAT, dans lequel un hôte source « interne » a initié une connexion IP avec un hôte cible « externe » via l'interface NAT et a converti une adresse source valide en interne en une adresse source valide en externe et un port source valide en externe. Valeurs possibles : • *full-cone* (uniquement UDP) : chaque hôte externe souhaité peut envoyer des paquets IP via l'adresse externe et le port externe à l'adresse source initiatrice et au port source initiateur. • *restricted-cone* (uniquement UDP) : comme full-cone NAT ; le seul hôte externe autorisé est toutefois l'hôte cible « externe » initial. • *port-restricted-cone* (uniquement UDP) : comme restricted-cone NAT ; seules sont toutefois autorisées les don-

Champ	Description
	nées du port cible initial. • *symétrique* (valeur par défaut) Pour les protocoles choisis : dans le sens sortant, une adresse source valide en externe et un port source valide en externe sont définis administrativement. Dans le sens entrant, seuls sont autorisés les paquets de réponse au sein de la connexion existante.

Le menu **Configuration NAT**->**Indiquer l'échange de données d'origine** permet de configurer pour quel échange de données NAT doit être utilisé.

Champs du menu Indiquer l'échange de données d'origine

Champ	Description
Service	Pas pour **Type d'échange de données** = *sortant (NAT source)*, ni **Méthode NAT** = *full-cone*, *restricted-cone* ou *port-restricted-cone*. Sélectionnez l'un des services préconfigurés. Valeurs possibles : • *Personnalisé* (valeur par défaut) • *<Nom de service>*
Action	Uniquement pour **Type d'échange de données** = *exclusif (sans NAT)* Sélectionnez quels paquets de données sont extraits par NAT. Valeurs possibles : • *Exclure* (valeur par défaut) : tous les paquets de données qui correspondent aux paramètres à configurer par la suite (protocole, adresse IP/masque de réseau source, adresse IP/masque de réseau cible, etc.) sont extraits par NAT. • *Ne pas exclure* : tous les paquets de données qui ne correspondent pas aux paramètres à configurer par la suite (protocole, adresse IP/masque de réseau source, adresse IP/masque de réseau cible, etc.) sont extraits par NAT.
Journal	Uniquement pour certains services. Pas pour **Type d'échange de données** = *sortant (NAT source)*, ni **Méthode NAT** = *full-cone*, *restricted-*

Champ	Description
	cone ou *port-restricted-cone*. Dans ce cas, UDP est défini automatiquement. Sélectionnez un protocole. Suivant le **Service** sélectionné, différents protocoles sont disponibles. Valeurs possibles : • *Quelconque* (valeur par défaut) • *AH* • *Chaos* • *EGP* • *ESP* • *GGP* • *GRE* • *HMP* • *ICMP* • *IGMP* • *IGP* • *IGRP* • *IP* • *IPinIP* • *IPv6* • *IPX in IP* • *ISO-IP* • *Kryptolan* • *L2TP* • *OSPF* • *PUP* • *RDP* • *RSVP* • *SKIP* • *TCP* • *TLSP* • *UDP*

Champ	Description
	• *VRRP* • *XNS-IDP*
Adresse IP source/ Masque de réseau	Uniquement pour **Type d'échange de données** = *entrant (NAT de destination)* ou *exclusif (sans NAT)* Saisissez les adresses IP source et, le cas échéant, les masques de réseau correspondants des paquets de données d'origine.
Adresse IP de destination originale/Masque de réseau	Uniquement pour **Type d'échange de données** = *entrant (NAT de destination)* Saisissez les adresses IP de destination et, le cas échéant, les masques de réseau correspondants des paquets de données d'origine.
Port de destination original/zone	Uniquement pour **Type d'échange de données** = *entrant (NAT de destination)*, **Service** = *personnalisé* et **Journal** = *TCP*, *UDP*, *TCP/UDP* Saisissez le port de destination ou la plage de ports de destination des paquets de données d'origine. Le paramètre par défaut *-Tous-* signifie que le port n'est pas spécifié de manière plus détaillée.
Adresse IP source originale/Masque de réseau	Uniquement pour **Type d'échange de données** = *sortant (NAT source)* Saisissez les adresses IP source et, le cas échéant, les masques de réseau correspondants des paquets de données d'origine.
Port source original/ zone	Uniquement pour **Type d'échange de données** = *sortant (NAT source)*, **Méthode NAT** = *symétrique*, **Service** = *personnalisé* et **Journal** = *TCP*, *UDP*, *TCP/UDP* Saisissez le port source des paquets de données d'origine. Le paramètre par défaut *-Tous-* signifie que le port n'est pas spécifié de manière plus détaillée. Lorsque vous sélectionnez *Saisir le port*, vous pouvez entrer un port unique. Lorsque vous sélectionnez *Saisir la plage de ports*, vous pouvez définir un domaine associé

Champ	Description
	aux ports, utilisé comme filtre pour l'échange des données sortantes.
Port source/zone	Uniquement pour **Type d'échange de données** = *exclusif (sans NAT)*, **Service** = *personnalisé* et **Journal** = *TCP*, *UDP*, *TCP/UDP* Saisissez le port source ou la plage de ports source des paquets de données d'origine. Le paramètre par défaut *-Tous-* signifie que le port n'est pas spécifié de manière plus détaillée.
Adresse IP de destination/Masque de réseau	Uniquement pour **Type d'échange de données** = *exclusif (sans NAT)* ou *sortant (NAT source)* et **Méthode NAT** = *symétrique* Saisissez les adresses IP de destination et, le cas échéant, les masques de réseau correspondants des paquets de données d'origine.
Port de destination/ zone	Uniquement pour **Type d'échange de données** = *sortant (NAT source)*, **Méthode NAT** = *symétrique*, **Service** = *défini par l'utilisateur* et **Journal** = *TCP*, *UDP*, *TCP/UDP* ou **Type d'échange de données** = *exclusif (sans NAT)*, **Service** = *défini par l'utilisateur* et **Journal** = *TCP*, *UDP*, *TCP/UDP* Saisissez le port de destination ou la plage de ports de destination des paquets de données d'origine. Le paramètre par défaut *-Tous-* signifie que le port n'est pas spécifié de manière plus détaillée.

Le menu **Configuration NAT**->**Valeur de substitution** permet, suivant qu'il s'agisse d'échange de données entrantes ou sortantes, de définir de nouveaux ports et adresses en lesquels sont convertis certains ports et adresses issus du menu **Configuration NAT**->**Indiquer l'échange de données d'origine**.

Champs du menu Valeur de substitution

Champ	Description
Nouvelle adresse IP de destination/Masque de réseau	Uniquement pour **Type d'échange de données** = *entrant (NAT de destination)* Saisissez l'adresse IP de destination et le masque de réseau

Champ	Description
	correspondant en lesquels doit être convertie l'adresse IP cible d'origine.
Nouveau port de destination	Uniquement pour **Type d'échange de données** = *entrant (NAT de destination)*, **Service** = *personnalisé* et **Journal** = *TCP*, *UDP*, *TCP/UDP* Quittez le port cible ou saisissez le port cible en lequel doit être converti le port cible d'origine. L'option *Original* permet de quitter le port cible d'origine. Lorsque vous désactivez *Original*, un champ de saisie apparaît et vous pouvez entrer un nouveau port cible. Par défaut, l'option *Original* est activée.
Nouvelle adresse IP source/Masque de réseau	Uniquement pour **Type d'échange de données** = *sortant (NAT source)* et **Méthode NAT** = *symétrique* Saisissez l'adresse IP source en laquelle doit être convertie l'adresse IP source d'origine, ainsi que le masque de réseau le cas échéant.
Nouveau port source	Uniquement pour **Type d'échange de données** = *sortant (NAT source)*, **Méthode NAT** = *symétrique*, **Service** = *personnalisé* et **Journal** = *TCP*, *UDP*, *TCP/UDP* Quittez le port source ou saisissez un nouveau port source en lequel doit être converti le port source d'origine. L'option *Original* permet de quitter le port source d'origine. Lorsque vous désactivez *Original*, un champ de saisie apparaît et vous pouvez entrer un nouveau port source. Par défaut, l'option *Original* est activée. Si pour **Port source original/zone** vous avez sélectionné *Saisir la plage de ports*, vous disposez des choix suivants : • *Utiliser port source / plage de ports sources originale*: la plage indiquée dans **Port source original/zone** n'est pas modifiée. Les numéros de ports sont conservés. • *Port/domaine utilisés en commençant par* : un

Champ	Description
	champ de saisie apparaît. Vous pouvez y entrer le numéro de port par lequel doit débuter la plage de ports , par laquelle la plage de ports d'origine est remplacée. Le nombre de ports reste inchangé.

10.3 QoS

QoS (Quality of Service) permet de répartir les bandes passantes disponibles intelligemment et efficacement. Certaines applications peuvent être favorisées et de la bande passante peut leur être réservée. Ceci représente un avantage particulièrement pour des applications critique, telles que VoIP.

La configuration QoS comporte trois parties :

- Définir le filtre IP
- Classifier les données
- Définir les priorités des données

10.3.1 Filtre QoS

Le menu **Réseau**->**QoS**->**Filtre QoS** permet de configurer les filtres IP.

La liste indique également toutes les entrées configurées depuis **Réseau**->**Règles d'accès**->**Chaînes de règles**.

10.3.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour définir d'autres filtres IP.

Le menu **Réseau**->**QoS**->**Filtre QoS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez la désignation du filtre.
Service	Sélectionnez l'un des services préconfigurés. D'origine, une liste complète de services est préconfigurée, dont : • *activity* • *apple-qt*

Champ	Description
	• *auth* • *chargen* • *clients_1* • *daytime* • *dhcp* • *discard* La valeur par défaut est *Personnalisé*.
Journal	Sélectionnez un protocole. L'option *Quelconque* (valeur par défaut) convient à tous les protocoles.
Type	Uniquement pour **Journal** = *ICMP* Sélectionnez un type. Valeurs possibles : *Quelconque*, *Echo reply*, *Destination unreachable*, *Source quench*, *Rediriger*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Voir la RFC 792. La valeur par défaut est *Quelconque*.
Etat de la connexion	Si **Journal** = *TCP*, vous pouvez définir un filtre qui tient compte de l'état des connexions TCP. Valeurs possibles : • *Etabli* : le filtre tient compte des paquets TCP qui n'ouvrent pas de nouvelle connexion TCP en cas de routage via la passerelle. • *Quelconque* (valeur par défaut) : Le filtre tient compte de tous les paquets TCP.
Adresse IP de destination/Masque de réseau	Saisissez les adresses IP de destination des paquets de données, ainsi que les masques de réseau correspondants.
Port de destination/ zone	Uniquement pour **Journal** = *TCP* ou *UDP* Saisissez un numéro de port de destination ou une plage de

Champ	Description
	numéros de ports de destination. Valeurs possibles : • *-Tous-* (valeur par défaut) : Le port de destination n'est pas spécifié de manière plus détaillée. • *Saisir le port* : saisissez un port de destination. • *Saisir la plage de ports* : saisissez une plage de ports de destination.
Adresse IP source/ Masque de réseau	Saisissez les adresses IP source des paquets de données, ainsi que les masques de réseau correspondants.
Port source/zone	Uniquement pour **Journal** = *TCP* ou *UDP* Saisissez un numéro de port source ou une plage de numéros de ports source. Valeurs possibles : • *-Tous-* (valeur par défaut) : Le port de destination n'est pas spécifié de manière plus détaillée. • *Saisir le port* : saisissez un port de destination. • *Saisir la plage de ports* : saisissez une plage de ports de destination.
Filtre DSCP/TOS (couche 3)	Sélectionnez le type de service (TOS, Type of Service). Valeurs possibles : • *Ignorer* (valeur par défaut) : Le type de service n'est pas pris en compte. • *Valeur binaire DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire, 6 bits). • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au for-

Champ	Description
	mat binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63. • *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F.
Filtre COS (802.1p/Layer 2)	Introduisez la classe de service des paquets IP (Class of Service, CoS). Les valeurs possibles sont des nombres entiers compris entre *0* et *7*. Plage de valeurs de *0* à *7*. La valeur par défaut est *Ignorer*.

10.3.2 Classification QoS

Le menu **Réseau**->**QoS**->**Classification QoS** permet de classifier l'échange de données : l'échange de données est affecté à différentes classes au moyen d'ID de classes. Vous créez pour cela des plans de classes pour le classement des paquets IP d'après les filtres IP définis précédemment. Au moins une interface est affectée à chaque plan de classes avec son premier filtre.

10.3.2.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres classes de données.

Le menu **Réseau**->**QoS**->**Classification QoS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Plan de classe	Sélectionné le plan de classes à créer ou éditer. Valeurs possibles : • *Nouveau* (valeur par défaut) : Ce paramètre vous permet de créer un nouveau plan de classes. • *<Nom du plan de classe>* : Indique un plan de classes déjà créé, que vous pouvez sélectionner et éditer. Vous pouvez ajouter de nouveaux filtres.

Champ	Description
Description	Uniquement pour **Plan de classe** = *Nouveau* Saisissez la désignation du plan de classes.
Filtre	Sélectionnez un filtre IP. Pour un nouveau plan de classes, sélectionnez le filtre qui doit être défini au premier plan du plan de classes. Pour un plan de classes existant, sélectionnez le filtre qui doit être associé au plan de classes. Pour pouvoir sélectionner un filtre, au moins un filtre doit être configuré dans le menu **Réseau**->**QoS**->**Filtre QoS**.
Sens	Sélectionnez le sens des paquets de données à classer. Valeurs possibles : • *Entrant* : la classe à définir par la suite (**ID de classe**) est affectée aux paquets de données entrants. • *Sortant* (valeur par défaut) : la classe à définir par la suite (**ID de classe**) est affectée aux paquets de données sortants. • *Les deux* : la classe à définir par la suite (**ID de classe**) est affectée aux paquets de données entrants et sortants.
Classe High-Priority	Activez ou désactivez la classe de haute priorité. Lorsque la classe de haute priorité est active, la classe avec la priorité la plus haute est affectée aux paquets de données. La priorité 0 est définie automatiquement. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
ID de classe	Uniquement pour **Classe High-Priority** pas actif. Sélectionnez un chiffre que le paquet de données affecte à une classe.

Champ	Description
	Note L'ID de classe est une étiquette permettant d'affecter les paquets de données à des classes définies. L'ID de classe ne définit aucune priorité. Les valeurs possibles sont des nombres entiers compris entre *1* et *254*.
Définir la valeur DSCP/ TOS (couche 3)	Vous pouvez définir ou modifier ici la valeur DSCP/TOS des paquets de données IP en fonction de la classe définie (**ID de classe**). Valeurs possibles : • *Reçu* (valeur par défaut) : La valeur DSCP/TOS des paquets de données reste inchangée. • *Valeur binaire DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire). • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au format binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63. • *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F.
Définir la valeur COS (802.1p/couche 2)	Vous pouvez définir ou modifier ici la classe de service (priorité de niveau 2) dans l'en-tête Ethernet VLAN des paquets IP en fonction de la classe définie (**ID de classe**). Les valeurs possibles sont des nombres entiers compris entre *0* et *7*.

Champ	Description
	La valeur par défaut est *Reçu*.
Interfaces	Uniquement pour **Plan de classe** = *Nouveau* Sélectionnez lors de la définition d'un nouveau plan de classes les interfaces auxquelles vous voulez associer le plan de classes. Un plan de classes peut être affecté à plusieurs interfaces.

10.3.3 Interfaces/Directives QoS

Vous définissez dans le menu **Réseau**->**QoS**->**Interfaces/Directives QoS** les priorités des données.

Note

Il n'est possible de définir des priorités que parmi les données sortantes.

Les paquets de la classe de priorité haute ont toujours la priorité sur les données avec l'ID de classe 1 - 254.

Il est possible d'affecter ou de garantir à chaque file d'attente et donc à chaque classe de données une proportion définie de la bande passante de l'interface. Vous pouvez par ailleurs optimiser la transmission des données vocales (données en temps réel).

Indépendamment de chaque interface, une file d'attente est créée automatiquement pour chaque classe, mais seulement pour l'échange de données sortantes et pour l'échange de données bidirectionnel. Une priorité est alors affectée aux files d'attente créées automatiquement. La valeur de priorité est égale à la valeur de l'ID de classe. Vous pouvez modifier la priorité définie par défaut pour une file d'attente. Lorsque vous ajoutez de nouvelles files d'attente, l'ID de classe permet d'utiliser aussi des classes d'autres plans.

10.3.3.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres priorités.

Le menu **Réseau**->**QoS**->**Interfaces/Directives QoS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Interface	Sélectionnez l'interface pour laquelle la QoS doit être configurée.
Algorithme de priorétisation	Sélectionnez l'algorithme suivant lequel les files d'attente doivent être gérées. Vous activez ou désactivez ainsi la QoS sur l'interface sélectionnée. Valeurs possibles : • *Priority Queueing* : QoS est activé sur l'interface. La bande passante disponible est répartie de manière précise en fonction de la priorité des files d'attente. • *Weighted Round Robin* : QoS est activé sur l'interface. La bande passante disponible est répartie en fonction du poids des files d'attente. Exception : Les paquets à priorité haute sont toujours traités avant les autres. • *Weighted Fair Queueing* : QoS est activé sur l'interface. La bande passante disponible est répartie de manière aussi « juste » que possible entre les connexions de données (identifiées automatiquement) au sein d'une file d'attente. Exception : Les paquets à priorité haute sont toujours traités avant les autres. • *Désactivé* (valeur par défaut) : QoS est désactivé sur l'interface. La configuration éventuellement présente n'est pas effacée et peut être de nouveau activée en cas de besoin.
Traffic Shaping	Activez ou désactivez une limitation du débit de données sortantes. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Vitesse de chargement maximale	Uniquement pour **Traffic Shaping** = activé. Entrez pour la file d'attente un débit maximal de données sortantes en kBits par seconde. Les valeurs possibles sont comprises entre *0* et *1000000*. La valeur par défaut est de *0* : aucune limitation, la file d'attente peut utiliser la bande passante maximale.

Champ	Description
Taille de l'en-tête du protocole sous la couche 3	Uniquement pour **Traffic Shaping** = activé. Sélectionnez le type d'interface pour tenir compte de la taille du surdébit d'un datagramme dans le calcul de la bande passante. Valeurs possibles : • *Personnalisé* Valeur en octet. Les valeurs possibles sont comprises entre *0* et *100*. • *Non défini (Protocol Header Offset=0)* (valeur par défaut) Sélection possible uniquement pour les interfaces Ethernet • *Ethernet* • *Ethernet et VLAN* • *PPP over Ethernet* • *PPPoE et VLAN* Sélection possible uniquement pour les interfaces IPSec • *IPSec via Ethernet* • *IPSec via Ethernet et VLAN* • *IPSec via PPP over Ethernet* • *IPSec via PPPoE et VLAN*
Méthode d'encryptage	Uniquement si IPSec Peer est sélectionné comme **Interface**, **Traffic Shaping** est *Activé* et la **Taille de l'en-tête du protocole sous la couche 3** n'est pas *Non défini (Protocol Header Offset=0).* Sélectionnez la méthode de cryptage utilisée pour la connexion IPSec. L'algorithme de cryptage détermine la longueur de chiffrement par blocs prise en considération pour le calcul de la bande passante. Valeurs possibles : • *DES, 3DES, Blowfish, Cast - (taille de chiffrement par blocs = 64 Bit)* • *AES128, AES192, AES256, Twofish - (taille de*

Champ	Description
	chiffrement par blocs = 128 Bit)
Real Time Jitter Control	Uniquement pour **Traffic Shaping** = activé Real Time Jitter Control entraîne une optimisation du comportement de latence lors de la transmission des datagrammes en temps réel. Cette fonction permet une fragmentation de grands paquets de données en fonction de la bande passante disponible en chargement. Real Time Jitter Control est utile avec de faibles bandes passantes en chargement (< 800 kBit/s). Activez ou désactivez Real Time Jitter Control. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Mode de contrôle	Uniquement pour **Real Time Jitter Control** = activé. Sélectionnez le mode pour l'optimisation de la transmission vocale. Valeurs possibles : • *Tous les RTP-Stream*: tous les flux RTP sont optimisés. La fonction active le mécanisme de détection de flux RTP pour l'identification automatique de flux RTP. Dans ce mode, le mécanisme Real-Time-Jitter-Control est actif dès l'identification d'un flux RTP. • *Inactif*: l'optimisation de la transmission des données vocales n'est pas effectuée. • *RTP-Stream contrôlés seulement* : ce mode est utilisé lorsque VoIP Application Layer Gateway (ALG) ou VoIP Media Gateway (MGW) est actif. L'activation du mécanisme Real-Time-Jitter-Control est réalisée avec les instances ALG ou MGW. • *Toujours* : le mécanisme Real-Time-Jitter-Control est toujours actif, même si aucune donnée en temps réel n'est routée.
Queues/Directives	Configurez les files d'attente QoS souhaitées.

Champ	Description
	Pour chaque classe définie dans le plan de classes et associée à l'interface souhaitée, une file d'attente est créée automatiquement et affichée ici (seulement pour l'échange de données sortantes et pour l'échange de données bidirectionnel). Ajoutez de nouvelles entrées à l'aide de l'option **Ajouter**. Le menu **Éditer Queue/Directive** apparaît. La création d'une directive QoS entraîne la création automatique d'une entrée par défaut DEFAULT avec la priorité la plus faible 255.

Le menu **Éditer Queue/Directive** se compose des champs suivants :

Champs du menu Éditer Queue/Directive

Champ	Description
Description	Saisissez la désignation de la file d'attente/directive.
Interface sortante	Indique l'interface pour laquelle les files d'attente QoS sont configurées.
Queue de priorétisation	Sélectionnez le type de gestion des priorités des files d'attente. Valeurs possibles : • *Basé sur les classes* (valeur par défaut) : file d'attente pour les données classées « normales ». • *Priorité élevée*: file d'attente pour les données classées « priorité haute ». • *Par défaut* : file d'attente pour les données non classées ou sans file d'attente définie pour leur classe.
ID de classe	Uniquement pour **Queue de priorétisation** = *Basé sur les classes* Sélectionnez la classe de paquet QoS pour laquelle cette file d'attente doit être utilisée. Pour cela, au moins un ID de classe doit avoir été entré dans le menu **Réseau**->**QoS**->**Classification QoS**.
Priorité	Uniquement pour **Queue de priorétisation** = *Basé sur les*

Champ	Description
	classes Sélectionnez la priorité de la file d'attente. Les valeurs possibles sont *1 (priorité haute)* à *254 (priorité basse)*. La valeur par défaut est *1*.
Pondération	Uniquement pour **Algorithme de priorétisation** = *Weighted Round Robin* ou *Weighted Fair Queueing* Sélectionnez la pondération de la file d'attente. Les valeurs possibles sont comprises entre *1* et *254*. La valeur par défaut est *1*.
Mode RTT (Realtime-Traffic-Modus)	Activez ou désactivez la transmission des données en temps réel. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Le mode RTT doit être activé pour les classes QoS dans lesquelles les données en temps réel sont prioritaires. Ce mode entraîne une amélioration du comportement de latence lors de la transmission des datagrammes en temps réel. Il est possible de configurer plusieurs files d'attente avec le mode RTT activé. Les files d'attente avec le mode RTT activé doivent toujours avoir une priorité supérieure aux files d'attente avec le mode RTT désactivé.
Traffic Shaping	Activez ou désactivez une limitation du débit de données sortantes (=Traffic Shaping). La limitation du débit de données est applicable à la file d'attente choisie. (Il ne s'agit pas de la limitation qui peut être définie au niveau de l'interface.) Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Vitesse de chargement maximale	Uniquement pour **Traffic Shaping** = activé.

Champ	Description
	Entrez pour la file d'attente un débit maximal de données sortantes en kBits par seconde. Les valeurs possibles sont comprises entre *0* et *1000000*. La valeur par défaut est *0*.
Surréservation autorisée	Uniquement pour **Traffic Shaping** = activé. Activez ou désactivez la fonction. Cette fonction régit le comportement de la limitation du débit de données. Lorsque la fonction **Surréservation autorisée** est activée, la limitation du débit de données définie pour une file d'attente peut être contournée, à condition de disposer de bande passante sur l'interface. Lorsque la fonction **Surréservation autorisée** est désactivée, la file d'attente ne peut jamais utiliser plus de bande passante que la limitation définie. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Taille de la salve (burst)	Uniquement pour **Traffic Shaping** = activé. Entrez le nombre maximal d'octets qui peuvent être ajoutés pendant une courte durée si le débit de données autorisé pour cette file d'attente est déjà atteint. Les valeurs possibles sont comprises entre *0* et *64000*. La valeur par défaut est *0*.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Algorithme Dropping	Sélectionnez le procédé suivant lequel des paquets sont placés dans la file d'attente QoS lorsque la taille maximale de la file d'attente est dépassée. Valeurs possibles :

Champ	Description
	• *Tail Drop* (valeur par défaut) : le nouveau paquet entrant est rejeté. • *Head Drop* : le plus ancien paquet dans la file d'attente est rejeté. • *Random Drop* : un paquet choisi au hasard est rejeté de la file d'attente.
Evitement de goulet d'étranglement (RED)	Activez ou désactivez l'effacement préventif des paquets de données. Les paquets de données de taille comprise entre **Taille Min. Queue** et **Taille Max. Queue** sont rejetés en priorité afin d'éviter un débordement de la file d'attente (RED = Random Early Detection). Avec un échange de données basé sur TCP, ce procédé permet d'avoir une plus petite file d'attente de manière à pouvoir même transmettre les salves de trafic sans perte importante de paquets. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Taille Min. Queue	Entrez le seuil inférieur en octets pour le procédé d'**évitement des blocages de données (RED)**. Les valeurs possibles sont comprises entre *0* et *262143*. La valeur par défaut est *0*.
Taille Max. Queue	Entrez le seuil supérieur en octets pour le procédé d'**évitement des blocages de données (RED)**. Les valeurs possibles sont comprises entre *0* et *262143*. La valeur par défaut est *16384*.

10.4 Règles d'accès

Les listes d'accès limitent les accès aux données et fonctions (quel utilisateur peut utiliser quels services et données).

Elles définissent des filtres pour les paquets IP afin d'autoriser ou bloquer l'accès depuis ou vers différents hôtes sur les réseaux connectés. Elles évitent ainsi l'établissement de

connexions non autorisées via la passerelle. Les listes d'accès définissent le type de trafic IP que la passerelle doit accepter ou refuser. La décision d'accès repose sur des informations contenues dans les paquets IP, par exemple :

- Adresse IP source et/ou cible
- Protocole du paquet
- Port source et/ou cible (les plages de ports sont prises en charge)

Si par exemple des sites dont les LAN sont connectés entre eux via une passerelle **Gigaset** veulent refuser toutes les demandes FTP entrantes, ou n'autoriser les sessions Telnet qu'entre certains hôtes, les listes d'accès constituent une méthode efficace.

Les filtres d'accès sur la passerelle reposent sur une combinaison de filtres et actions sur les règles de filtres (= rules) et sur l'association de ces règles à des chaînes de règles. Ils agissent sur les paquets de données entrants et peuvent ainsi accorder ou refuser l'accès à la passerelle à certaines données.

Un filtre décrit une partie données de l'échange de données IP en fonction des adresses IP source et/ou cible, du masque de réseau, du protocole et du port source et/ou cible.

Les règles organisées en listes d'accès permettent d'indiquer à la passerelle comment traiter les paquets de données filtrés (les accepter ou les refuser). Vous pouvez également définir plusieurs règles organisées sous forme d'une chaîne, dans un ordre donné.

Il existe plusieurs approches pour la définition de règles ou de chaînes de règles :

Accepter tous les paquets qui ne sont pas exclus explicitement :

- Rejeter tous les paquets qui correspondent au filtre 1.
- Rejeter tous les paquets qui correspondent au filtre 2.
- ...
- Laisser passer le reste.

ou

N'accepter que les paquets qui sont explicitement autorisés :

- Accepter tous les paquets qui correspondent au filtre 1.
- Accepter tous les paquets qui correspondent au filtre 2.
- ...
- Rejeter le reste.

ou

Combinaison des deux possibilités décrites ci-dessus.

Plusieurs chaînes de règles distinctes peuvent être créées. Il est alors possible d'utiliser simultanément des filtres dans différentes chaînes de règles.

Vous pouvez affecter une chaîne de règles à chaque interface individuellement.

Attention

Veillez à ne pas vous bloquer vous-même lors de la configuration des filtres :

Accédez à la configuration des filtres, si possible depuis l'interface de console série ou par connexion RNIS à votre passerelle.

10.4.1 Filtre d'accès

Ce menu permet de configurer les filtres d'accès. Chaque filtre décrit une partie donnée du trafic IP, et définit par exemple les adresses IP, le protocole et le porte source ou cible.

Le menu **Réseau**->**Règles d'accès**->**Filtre d'accès** permet d'afficher une liste de tous les filtres d'accès.

10.4.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer les filtres d'accès.

Le menu **Réseau**->**Règles d'accès**->**Filtre d'accès**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une désignation pour le filtre.
Service	Sélectionnez l'un des services préconfigurés. D'origine, une liste complète de services est préconfigurée, dont : • *activity* • *apple-qt* • *auth* • *chargen*

Champ	Description
	• *clients_1* • *daytime* • *dhcp* • *discard* La valeur par défaut est *Personnalisé*.
Journal	Sélectionnez un protocole. L'option *Quelconque* (valeur par défaut) convient à tous les protocoles.
Type	Uniquement si **Journal** = *ICMP* Valeurs possibles : • *Quelconque* • *Echo reply* • *Destination unreachable* • *Source quench* • *Rediriger* • *Echo* • *Time exceeded* • *Timestamp* • *Timestamp reply* La valeur par défaut est *Quelconque*. Voir la RFC 792.
Etat de la connexion	Uniquement si **Journal** = *TCP* Vous pouvez définir un filtre qui tient compte de l'état de la connexion TCP. Valeurs possibles : • *Quelconque* (valeur par défaut) : Le filtre tient compte de tous les paquets TCP. • *Etabli* : le filtre tient compte des paquets TCP qui n'ouvrent pas de nouvelle connexion TCP en cas de routage via la

Champ	Description
	passerelle.
Adresse IP de destination/Masque de réseau	Définissez l'adresse IP cible et le masque de réseau des paquets de données. Valeurs possibles : • *Quelconque* (valeur par défaut) • *Hôte* : saisissez l'adresse IP de l'hôte. • *Réseau* : saisissez l'adresse réseau et le masque de réseau correspondant.
Port de destination/ zone	Uniquement si **Journal** = *TCP*, *UDP* Saisissez un numéro de port de destination ou une plage de numéros de ports de destination sur laquelle le filtre convient. Valeurs possibles : • *-Tous-* (valeur par défaut) : Le filtre est valable pour tous les numéros de ports. • *Saisir le port* : permet la saisie d'un numéro de port. • *Saisir la plage de ports* : permet la saisie d'une plage de numéros de ports.
Adresse IP source/ Masque de réseau	Saisissez l'adresse IP source et le masque de réseau des paquets de données.
Port source/zone	Uniquement si **Journal** = *TCP*, *UDP* Saisissez le numéro de port source ou la plage de numéros de ports source. Valeurs possibles : • *-Tous-* (valeur par défaut) : Le filtre est valable pour tous les numéros de ports. • *Saisir le port* : permet la saisie d'un numéro de port. • *Saisir la plage de ports* : permet la saisie d'une plage de numéros de ports.
Filtre DSCP/TOS (couche 3)	Sélectionnez le type de service (TOS, Type of Service). Valeurs possibles :

Champ	Description
	• *Ignorer* (valeur par défaut) : Le type de service n'est pas pris en compte. • *Valeur binaire DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire, 6 bits). • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au format binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63. • *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F.
Filtre COS (802.1p/Layer 2)	Introduisez la classe de service des paquets IP (Class of Service, CoS). Les valeurs possibles sont des nombres entiers compris entre *0* et *7*. La valeur par défaut est *Ignorer*.

10.4.2 Chaînes de règles

Le menu **Chaînes de règles** permet de configurer les règles pour les filtres IP. Ils peuvent être créés individuellement ou associés dans des chaînes de règles.

Le menu **Réseau**->**Règles d'accès**->**Chaînes de règles** permet d'afficher la liste de toutes les règles de filtres créées.

10.4.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer les listes d'accès.

Le menu **Réseau**->**Règles d'accès**->**Chaînes de règles**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Chaîne de règle	Indiquez si vous souhaitez créer une chaîne de règle ou en éditer une existante. Valeurs possibles : • *Nouveau* (valeur par défaut) : Ce paramètre vous permet de créer une chaîne de règle. • *<Nom du plan de classe>* : Sélectionnez une chaîne de règles déjà créée et ajoutez une règle supplémentaire.
Description	Saisissez la désignation de la chaîne de règle.
Filtre d'accès	Sélectionnez un filtre IP. Pour une nouvelle chaîne de règle, sélectionnez le filtre qui doit être défini au premier plan de la chaîne de règle. Pour une chaîne de règle existante, sélectionnez le filtre qui doit être associé à la chaîne de règle.
Action	Déterminez la procédure à suivre avec un paquet de données filtré. Valeurs possibles : • *Autoriser si le filtre est adapté* (valeur par défaut) : accepter le paquet lorsque le filtre convient. • *Autoriser si le filtre n'est pas adapté* : accepter le paquet lorsque le filtre ne convient pas. • *Interdire si le filtre est adapté* : rejeter le paquet lorsque le filtre convient. • *Interdire si le filtre ne correspond pas* : rejeter le paquet lorsque le filtre ne convient pas. • *Ignorer* : appliquer la règle suivante.

Pour modifier l'ordre des règles d'une chaîne, sélectionnez dans le menu de liste le bouton pour l'entrée à déplacer. Une boîte de dialogue apparaît, et permet de décider sous **Déplacer** si l'entrée *sous* (valeur par défaut) ou *via* déplacera un autre règle de cette

chaîne.

10.4.3 Affectation des interfaces

Ce menu permet d'affecter les chaînes de règles configurées aux différentes interfaces et de définir le comportement de la passerelle lors du rejet de paquets IP.

Le menu **Réseau**->**Règles d'accès**->**Affectation des interfaces** présente une liste de toutes les affectations d'interfaces configurées.

10.4.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer d'autres affectations.

Le menu **Réseau**->**Règles d'accès**->**Affectation des interfaces**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Interface	Sélectionnez l'interface à laquelle attribuer une chaîne de règle configurée.
Chaîne de règle	Sélectionnez une chaîne de règle.
Rejet sans notification	Définissez si l'émetteur doit être informé en cas de rejet du paquet IP. • *Activé* (valeur par défaut) : l'émetteur n'est pas informé. • *Désactivé* : l'émetteur reçoit une notification ICMP.
Méthode de compte-rendu	Définissez si un message Syslog doit être créé en cas de rejet d'un paquet IP. Valeurs possibles : • *Pas de rapport* : aucun message Syslog. • *Info* (valeur par défaut) : un message Syslog est généré, avec indication du numéro de protocole, de l'adresse IP source et du numéro de port source. • *Dump* : un message Syslog est généré, avec le contenu des 64 premiers octets du paquet rejeté.

10.5 Drop-In

Le mode Drop-In permet de diviser un réseau en plusieurs segments sans avoir à séparer le réseau IP en sous-réseaux. Plusieurs interfaces peuvent être rassemblées en un groupe Drop-In et affectées à un réseau. Toutes les interfaces sont alors configurées avec la même adresse IP.

Les composants réseau d'un segment liés à une connexion peuvent alors par exemple être protégés ensemble avec un pare-feu. L'échange de données de composants réseau entre différents segments affectés à différents ports est ainsi contrôlé en fonction des règles de pare-feu configurées.

10.5.1 Groupes Drop-In

Le menu **Réseau**->**Drop-In**->**Groupes Drop-In** permet d'afficher une liste de tous les **Groupes Drop-In**. Un groupe **Drop-In** représente un réseau.

10.5.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour établir de nouveaux **Groupes Drop-In**.

Le menu **Réseau**->**Drop-In**->**Groupes Drop-In**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description du groupe	Saisissez une désignation claire pour le groupe **Drop-In**.
Mode	Sélectionnez le mode à utiliser pour la transmission des adresses MAC des composants réseau. Valeurs possibles : • *Transparent* (valeur par défaut) : les paquets ARP et les paquets IP correspondant au réseau Drop-In sont transmis de manière transparente (sans modification). • *Proxy* : les paquets ARP et les paquets IP correspondant au réseau Drop-In sont transmis avec l'adresse MAC de l'interface correspondante.
Configuration réseau	Sélectionnez de quelle manière un masque de réseau ou une

Champ	Description
	adresse IP sont affectés au réseau **Drop-In**. Valeurs possibles : • *Statique* (valeur par défaut) • *DHCP*
Adresse réseau	Uniquement pour **Configuration réseau** = *Statique* Saisissez l'adresse du réseau **Drop-In**.
Masque réseau	Uniquement pour **Configuration réseau** = *Statique* Indiquez le masque de réseau correspondant.
Adresse IP locale	Uniquement pour **Configuration réseau** = *Statique* Saisissez l'adresse IP locale. Cette adresse IP doit être identique pour tous les ports Ethernet d'un réseau.
Client DHCP sur l'interfaces	Uniquement pour **Configuration réseau** = *DHCP* Vous pouvez sélectionner ici une interface Ethernet de votre routeur devant agir comme client DHCP. Vous avez par exemple besoin de ce paramètre lorsque le routeur de votre fournisseur doit servir de serveur DHCP. Vous avez le choix entre les interfaces mises à disposition par votre appareil. L'interface doit toutefois être membre du groupe Drop-In.
ARP Lifetime	Définit la période sur laquelle les entrées ARP doivent être conservées dans le cache. La valeur par défaut est *3600* secondes.
Affectation DNS via DHCP	La passerelle peut modifier les paquets DHCP qui parcourent le groupe Drop-In et s'entrer elle-même comme serveur de DNS proposé. Valeurs possibles : • *Inchangé* (valeur par défaut) • *Adresse IP propre*

Champ	Description
Exclure du NAT (DMZ)	Vous pouvez extraire ici l'échange de données du NAT. Utilisez par exemple cette fonction pour garantir l'accès à des serveurs Web donnés au sein d'une ZDM. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Sélection interfaces	Sélectionnez tous les ports à inclure dans le groupe **Drop-In** (sur le réseau). Ajoutez d'autres entrées à l'aide de l'option **Ajouter**.

Chapitre 11 Multicast

Qu'est-ce que la multidiffusion ?

De nombreuses technologies de communication récentes reposent sur la communication depuis un émetteur vers plusieurs destinataires. Il est donc important de veiller à la réduction de l'échange de données des systèmes de télécommunications modernes, tels que Voice-over-IP ou le streaming vidéo et audio (par exemple télévision IP ou webradio), par exemple dans le cadre du TriplePlay (voix, vidéo, données). La multidiffusion propose une solution abordable pour une utilisation efficace de la bande passante, afin que l'émetteur n'ait besoin d'envoyer qu'une fois le paquet de données, qui pourra être reçu par plusieurs destinataires. Le paquet est donc envoyé vers une adresse virtuelle, nommée groupe de multidiffusion. Les destinataires intéressés se connectent à ce groupe.

Autres domaines d'utilisation

Un domaine d'utilisation classique de la multidiffusion correspond aux conférences (audio/vidéo) avec plusieurs destinataires. Les plus connus doivent être MBone Multimedia Audio Tool (VAT), Video Conferencing Tool (VIC) et le Whiteboard (WB). VAT permet de réaliser des conférences audio. Tous les interlocuteurs sont pour cela affichés dans une fenêtre et le ou les intervenants sont identifiés par un cadre noir. Les autres domaines d'utilisation intéressent principalement les entreprises. La multidiffusion permet de synchroniser simultanément les bases de données de plusieurs serveurs, ce qui est très utiles pour les multinationales ainsi que pour les entreprises qui ne comptent que quelques établissements.

Plage d'adresses pour la multidiffusion

Les adresses IP 224.0.0.0 à 239.255.255.255 (224.0.0.0/4) sur le réseau de classe D sont réservées à la multidiffusion pour IPv4. Une adresse IP sur cette plage représente un groupe de multidiffusion, auquel plusieurs destinataires peuvent se connecter. Le routeur de multidiffusion transmet alors les paquets souhaités vers tous les sous-réseaux avec les destinataires connectés.

Conditions pour la multidiffusion

La multidiffusion est un système sans connexion : tout contrôle de flux ou correction d'erreur doit être garanti au niveau de l'application.

Au niveau du transport, on n'utilise presque que l'UDP, car contrairement au TCP, ce protocole n'est pas associé à une liaison point à point.

La principale différence se situe au niveau IP, car l'adresse cible ne désigne aucun hôte dédié, mais est destinée à un groupe : lors du routage de paquets de multidiffusion, tout dépend de la présence d'un destinataire sur un sous-réseau connecté.

Sur le réseau local, tous les hôtes doivent accepter tous les paquets de multidiffusion. Avec Ethernet ou FDD, cela repose sur un mappage MAC, les différentes adresses de groupes étant codées dans l'adresse MAC de destination. Pour le routage entre plusieurs réseaux, les différents routeurs doivent d'abord connaître tous les destinataires potentiels sur le sous-réseau. On utilise pour cela un protocole de gestion des membres, tel qu'IGMP pour IPv4 et MLP pour IPv6.

Protocole de gestion des membres

IGMP (Internet Group Management Protocol) est un protocole dans IPv4 permettant aux hôtes de transmettre au routeur des informations sur les membres de la multidiffusion. L'adressage repose sur les adresses IP de la classe D. Une adresse IP de cette classe représente un groupe. Un émetteur (par exemple une Webradio) émet vers ce groupe. Les adresses (IP) des différents émetteurs au sein d'un groupe sont désignées comme adresses source. Plusieurs émetteurs (avec des adresses IP différentes) peuvent ainsi émettre vers le même groupe de multidiffusion. Il s'agit d'une relation 1 à n entres les adresses du groupe et source. Ces informations sont transmises au routeur au moyen de rapports. Lors de la réception de données de multidiffusion, un routeur peut utiliser ces informations pour déterminer si un hôte sur un sous-réseau les recevra ou non. Votre appareil prend en charge la version actuelle IGMP V3, qui est compatible en amont : les hôtes V3, V1 et V2 peuvent être gérés.

Votre appareil prend en charge les mécanismes de multidiffusion suivants :

- Forwarding (transmission) : il s'agit là d'une transmission statique : les données entrantes pour un groupe sont transmises dans tous les cas. Ce mode est adapté aux besoins de transmission permanente des données de multidiffusion.
- IGMP : ce protocole regroupe les informations sur les destinataires potentiels sur un sous-réseau. Dans le cas d'un bond, cela permet de sélectionner les données de multidiffusion entrantes.

Tuyau

L'essentiel en matière de diffusion consiste à exclure de l'échange de données les groupes de diffusion indésirables. Lors d'une association du transfert avec l'IGMP, les paquets peuvent toujours être transmis vers les groupes indiqués pour le transfert.

11.1 Général

11.1.1 Général

Le menu **Multicast**->**Général**->**Général** permet d'activer ou désactiver la fonction de multidiffusion.

Le menu **Multicast**->**Général**->**Général** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Routage multicast	Indiquez si **Routage multicast** doit être utilisé. Sélectionnez `Activé` pour activer la fonction. La fonction est désactivée par défaut.

11.2 IGMP

Le protocole IGMP (Internet Group Management Protocol, voir RFC 3376) permet de signaler les informations sur les groupes (appartenance) dans un sous-réseau. Ainsi, le sous-réseau ne reçoit que les paquets souhaités explicitement par un hôte.

Des mécanismes spécifiques permettent d'unifier les souhaits des différents clients. Il existe actuellement trois versions d'IGMP (V1 à V3). Les systèmes actuels utilisent en majorité V3, et plus rarement V2.

Deux types de paquets jouent un rôle central dans le protocole IGMP : requêtes et rapports.

Les requêtes sont exclusivement envoyées par un routeur. S'il existe plusieurs routeurs IGMP sur un réseau, le routeur avec l'adresse IP la plus basse envoie les requêtes. Il convient de différencier la requête générale (envoyée à 224.0.0.1), la requête spécifique au groupe (envoyée à une adresse de groupe) et la requête spécifique au groupe et à la source (envoyée à une adresse de groupe). Les rapports ne sont envoyés par des hôtes que pour répondre à des requêtes.

11.2.1 IGMP

Ce menu permet de confiture les interfaces sur lesquels IGMP doit être actif.

11.2.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Sélectionnez le bouton **Nouveau** pour configurer IGMP sur d'autres interfaces.

Le menu **Multicast**->**IGMP**->**IGMP**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres IGMP

Champ	Description
Interface	Sélectionnez l'interface sur laquelle IGMP doit être activé : les requêtes sont envoyées et les réponses activées.
Intervalle d'interrogation	Entrez l'intervalle en secondes sur lequel des requêtes IGMP doivent être envoyées. Les valeurs possibles sont comprises entre *0* et *600*. La valeur par défaut est *125*.
Temps de réponse maximal	Indiquez l'intervalle en secondes pendant lequel les hôtes doivent systématiquement répondre aux requêtes envoyées. Les hôtes choisissent parmi cet intervalle un délai avant l'envoi de la réponse. Cela permet de réaliser une dispersion et donc de décharger les réseaux contenant de nombreux hôtes. Les valeurs possibles sont comprises entre *0,0* et *25,0*. La valeur par défaut est *10,0*.
Solidité	Sélectionnez le multiplicateur pour la dispersion des valeurs de temporisation interne. Une valeur élevée permet par exemple de compenser la perte de paquets sur un réseau avec des pertes élevées. Une valeur excessive augmente toutefois la durée entre la déconnexion et l'arrêt de l'entrée de données (Leave Latency). Les valeurs possibles sont comprises entre *2* et *8*. La valeur par défaut est *2*.
Intervalle de réponse (dernier membre)	Déterminez combien de temps le routeur attend une réponse après une requête à un groupe. Une réduction de la valeur permet de déterminer plus vite si le

Champ	Description
	dernier membre a quitté un groupe et donc s'il ne faut plus transmettre aucun paquet à l'interface pour ce groupe. Les valeurs possibles sont comprises entre *0,0* et *25,0*. La valeur par défaut est *1,0*.
Nombre maximal de messages d'état IGMP	Limitez le nombre de rapports/requêtes par seconde pour l'interface sélectionnée.
Mode	Sélectionnez si l'interface définie ici fonctionne uniquement en mode hôte ou aussi en mode de routage. Valeurs possibles : • *Routage* (valeur par défaut) : L'interface est utilisée en mode de routage. • *Hôte*: l'interface n'est utilisée qu'en mode hôte.

IGMP Proxy

IGMP Proxy permet de simuler plusieurs interfaces connectées en local comme un sous-réseau à un routeur voisin. Les requêtes qui entrent sur l'interface IGMP Proxy sont transmises vers les sous-réseaux locaux. Les rapports locaux sont transmis à 'interface IPGM Proxy.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
IGMP Proxy	Définissez ici si votre appareil doit transmettre les messages IGMP des hôtes dans le sous-réseau via son **Interface proxy** définie.
Interface proxy	Uniquement pour **IGMP Proxy** = activé Sélectionnez l'interface de votre appareil, sur laquelle les requêtes doivent être acceptées et regroupées.

11.2.2 Options

Ce menu permet d'activer ou désactiver IGMP sur votre système. Vous pouvez également déterminer si IGMP doit être utilisé en mode de compatibilité ou si seuls les hôtes V3 IGMP doivent être acceptés.

Le menu **Multicast**->**IGMP**->**Options** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
État IGMP	Sélectionnez le statut IGMP. Valeurs possibles : • *Auto* (valeur par défaut) : La multidiffusion est automatiquement activée pour les hôtes. Utiliser la multidiffusion lors de l'ouverture de ces applications. • *Actif*: la multidiffusion est toujours active. • *Inactif*: la multidiffusion est toujours inactive.
Mode	Uniquement pour **État IGMP** = *Actif* ou *Auto* Sélectionnez le mode de multidiffusion. Valeurs possibles : • *Mode de compatibilité* (valeur par défaut) : Le routeur utilise IGMP version 3. S'il détecte une version inférieure sur le réseau, il utilise la version la plus basse qu'il peut détecter. • *Uniquement version 3*: seul IGMP version 3 est utilisé.
Groupes maxi	Entrez le nombre maximal de groupes possible en interne et dans les rapports.
Sources maxi	Entrez le nombre maximal de sources spécifiées dans les rapports dans la version 3 et le nombre maximal de sources gérées en interne par groupe.
Nombre maximal de messages d'état IGMP	Entrez le nombre maximal de requêtes ou de messages entrants possibles par seconde. La valeur par défaut est de *0* : le nombre de messages d'état

Champ	Description
	IGMP n'est pas limité.

11.3 Transférer

11.3.1 Transférer

Vous définissez dans ce menu quels groupes de multidiffusion sont toujours transmis entre les interfaces de votre appareil.

11.3.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour créer des règles de transfert pour les nouveaux groupes de multidiffusion.

Le menu **Multicast**->**Transférer**->**Transférer**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Tous les groupes multicast	Déterminez si tous les groupes de multidiffusion (l'ensemble de l'espace d'adresses de multidiffusion 224.0.0.0/4) doivent être transmis de l'**Interface source** définie à l'**Interface de destination** définie. Cochez pour cela *Activé*. Si vous ne voulez transmettre qu'un groupe de multidiffusion défini vers une interface donnée, désactivez l'option. L'option est désactivée par défaut.
Adresse groupes multicast	Uniquement pour **Tous les groupes multicast** = pas actif Entrez ici l'adresse du groupe de multidiffusion que vous voulez transmettre d'une **Interface source** définie vers une **Interface de destination** définie.
Interface source	Sélectionnez l'interface de votre appareil sur laquelle arrive le groupe de multidiffusion souhaité.
Interface de destination	Sélectionnez l'interface de votre appareil vers laquelle le groupe de multidiffusion souhaité doit être transféré.

Chapitre 12 WAN

Ce menu vous propose plusieurs possibilités pour la configuration de vos accès ou connexions LAN en WAN. Vous pouvez en outre y optimaliser la transmission vocale pour les conversations téléphoniques via Internet.

12.1 Internet + composer

Ce menu permet de configurer les accès Internet ou les connexions d'entrée.

De plus, vous pouvez créer des pools d'adresses pour l'attribution dynamique d'adresses IP.

Afin de pouvoir établir avec votre appareil des connexions à des réseaux ou des hôtes extérieurs à votre LAN, vous devez configurer le partenaire de communication souhaité sur votre appareil. Cela vaut tant pour les connexions sortantes (p. ex. lorsque votre appareil se connecte à un partenaire distant) qu'entrantes (p. ex. lorsqu'un partenaire distant se connecte à votre appareil).

Si vous souhaitez définir un accès à Internet, vous devez établir une connexion à votre fournisseur d'accès Internet (ISP). Pour les accès Internet à large bande, votre appareil propose les protocoles PPP-over-Ethernet (PPPoE), PPP-over-PPTP et PPP-over-ATM (PPPoA). Un accès Internet via RNIS peut également être configuré.

Note

Tenez compte des paramètres propres à votre fournisseur !

Les connexions d'entrée via RNIS servent à établir une connexion à des réseaux ou hôtes extérieurs à votre LAN.

Toutes les connexions entrées sont affichées dans la liste correspondante contenant la **Description**, le **Nom de l'utilisateur**, l'**Authentification** et l'**État** actuel.

Le champ **État** peut contenir les valeurs suivantes :

Valeurs possibles pour État

Champ	Description
	connecté
	non connecté (communications téléphoniques) ; établissement d'une connexion possible

Champ	Description
	non connecté (p. ex. en raison d'une erreur durant l'établissement d'une connexion sortante, une nouvelle tentative n'est possible qu'après un nombre déterminé de secondes)
	administratif désactivé ; établissement d'une connexion impossible

Route par défaut (Default Route)

En cas de route par défaut, toutes les données sont automatiquement transmises vers une connexion, si aucune autre route adaptée n'est disponible. Un accès à Internet doit toujours être configuré comme route par défaut à votre fournisseur d'accès Internet (ISP). Vous trouverez des informations plus détaillées concernant les types de routes possibles dans **Réseau**->**Routes**.

Activer le NAT

Le NAT (Network Address Translation) permet de dissimuler votre réseau tout entier derrière une seule adresse IP. Pour la connexion à votre fournisseur d'accès Internet (ISP), il est vivement conseillé de le faire.

Une fois le NAT activé, seules des sessions sortantes sont tout d'abord permises. Afin de permettre des connexions précises provenant de l'extérieur à des hôtes au sein du LAN, celles-ci doivent être explicitement définies et autorisées.

Définir le Timeout en cas d'inactivité

Le Timeout en cas d'inactivité est défini pour l'interruption automatique de la connexion en cas de non-utilisation, c'est-à-dire lorsque plus aucunes données utiles ne sont envoyées, permettant ainsi l'économie de frais, le cas échéant.

Bloquer après erreur de connexion

Cette fonction permet de configurer un temps d'attente pour les tentatives de connexions sortantes après l'échec d'une tentative par votre appareil.

Authentification

En cas d'appel entrant par des connexions RNIS, le numéro de l'appelant est communiqué par le canal D RNIS. A l'aide de ce numéro, votre appareil peut identifier l'appelant (CLID) si ce dernier est entré sur votre appareil. Après l'identification par CLID, votre ap-

pareil peut exécuter une authentification PPP supplémentaire avec le partenaire de communication avant d'accepter l'appel.

Pour toutes les connexions PPP, votre appareil nécessite la saisie de données de comparaison. Déterminez la négociation d'autorisation devant être effectuée et saisissez un mot de passe commun et deux numéros d'identification. Vous recevez p. ex. ces données de votre fournisseur d'accès Internet ou de l'administrateur système du siège de la société. Si les données saisies par vos soins sur votre appareil correspondent à celles de l'appelant, l'appel est accepté. Si les données ne correspondent pas, l'appel est refusé.

Callback

Afin d'acquérir une sécurité supplémentaire concernant le partenaire de communication, ou de pouvoir répartir clairement les frais de connexions, le mécanisme Callback peut être utilisé pour chaque connexion via une interface RNIS ou AUX. De la sorte, une connexion n'est établie que par un rappel, une fois l'appelant clairement identifié. Votre appareil peut tout aussi bien répondre à un appel entrant par un rappel, que d'exiger un rappel d'un partenaire de communication. L'identification peut être effectuée sur la base du Calling Party Number ou de l'authentification PAP/CHAP/MS-CHAP. Dans le premier cas, l'identification s'effectue sans prise d'appel, puisque le Calling Party Number est transmis via le canal D RNIS, dans le deuxième, avec prise d'appel.

Groupage des canaux

Votre appareil prend en charge le groupage dynamique et statique des canaux pour les communications téléphoniques. Le groupage des canaux ne peut être utilisé que pour les connexions RNIS pour l'augmentation de la bande passante, ou en tant que sauvegarde. Lors de l'établissement d'une communication, seul un canal B est ouvert dans un premier temps.

Dynamique

Le groupage dynamique des canaux signifie que l'appareil, au besoin, c'est-à-dire en cas de débits de données importants, ouvre des canaux B RNIS supplémentaires pour les connexions afin d'augmenter le débit. Si le flux de données diminue, les canaux B supplémentaires se ferment de nouveau.

Si le dispositif utilise des appareils d'autres fabricants, vérifiez que ceux-ci prennent en charge le groupage dynamique des canaux pour l'augmentation de la bande passante, ou en tant que sauvegarde.

Statique

Avec le groupage statique des canaux, vous déterminez au préalable le nombre de ca-

naux B à utiliser par votre appareil pour les connexions, indépendamment des débits de données transmises.

12.1.1 PPPoE

Le menu **WAN**->**Internet + composer**->**PPPoE** affiche la liste de toutes les interfaces PPPoE.

PPP over Ethernet (PPPoE) est l'utilisation du protocole de réseau Point-to-Point Protocol (PPP) via une connexion Ethernet. Le protocole PPPoE est aujourd'hui utilisé pour les connexions ADSL en Allemagne. En Autriche, le protocole Point To Point Tunneling Protocol (PPTP) était initialement utilisé pour les connexions ADSL. Aujourd'hui toutefois, le protocole PPPoE y est aussi offert par quelques fournisseurs.

12.1.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres interfaces PPPoE.

Le menu **WAN**->**Internet + composer**->**PPPoE**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez un nom pour désigner clairement le partenaire PPPoE. Dans ce champ, le premier caractère ne peut pas être un chiffre. Les caractères spéciaux et trémas ne peuvent pas non plus être utilisés.
Mode PPPoE	Indiquez si vous utilisez une connexion Internet par défaut via PPPoE (*Par défaut*) ou si votre accès Internet doit être établi via plusieurs interfaces (*Connexion multiple*). En choisissant *Connexion multiple*, vous pouvez coupler plusieurs connexions DSL d'un fournisseur via le protocole PPP en tant que groupage statique afin d'obtenir plus de bande passante. Chacune de ces connexions DSL doit utiliser pour ce faire une connexion Ethernet séparée. La fonction PPPoE Multilink est actuellement seulement en préparation chez de nombreux fournisseurs. Nous vous conseillons pour le PPPoE Multilink d'exploiter le commutateur Ethernet de votre appareil en mode Split Port et d'utiliser pour chaque connexion PPPoE une interface Ethernet

Champ	Description
	propre, p. ex. *en1-1*, *en1-2*. Si vous souhaitez utiliser pour le PPPoE Multilink un modem externe supplémentaire, vous devez exploiter le commutateur Ethernet de votre appareil en mode Split Port.
Interface Ethernet-PPPoE	Uniquement pour **Mode PPPoE** = *Par défaut* Sélectionnez l'interface Ethernet définie par défaut pour une connexion PPPoE standard. En cas d'utilisation d'un modem DSL externe, sélectionnez ici le port Ethernet auquel le modem est raccordé. En cas d'utilisation du modem DSL interne, sélectionnez l'interface EthoA configurée pour cette connexion dans **WAN**->**ATM**->**Profils**->**Nouveau**.
interface PPPoE pour liaison multiple	Uniquement pour **Mode PPPoE** = *Connexion multiple* Sélectionnez toutes les interfaces que vous souhaitez utiliser pour votre connexion Internet. Cliquez sur le bouton **Ajouter** pour créer des entrées supplémentaires.
Nom de l'utilisateur	Saisissez le nom d'utilisateur.
Mot de passe	Saisissez le mot de passe.
VLAN	Certains fournisseurs d'accès Internet exigent un identificateur de VLAN. Activez cette fonction afin de pouvoir entrer une valeur sous **ID VLAN**.
ID VLAN	Uniquement si **VLAN** est activé. Saisissez l'identificateur de VLAN que vous avez reçu de votre fournisseur.
Toujours actif	Indiquez si l'interface doit être activée en permanence. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. N'activez cette option que si vous disposez d'un accès Internet

Champ	Description
	avec un forfait fixe.
Timeout en cas d'inactivité	Uniquement si **Toujours actif** est désactivé. Saisissez l'intervalle d'inactivité en secondes pour le shorthold statique. Vous définissez ainsi le nombre de secondes devant s'écouler entre l'envoi du dernier paquet de données et la déconnexion. Valeurs possibles comprises entre *0* et *3600* (secondes). *0* permet de désactiver le shorthold. La valeur par défaut est *300*. Ex. *10* pour les transmissions FTP, *20* pour les transmissions de LAN à LAN, *90* pour les connexions Internet.

Champs du menu Mode IP et routes

Champ	Description
Mode Adresse IP	Indiquez si une adresse IP statique ou dynamique doit être affectée à votre appareil. Valeurs possibles : • *Appeler l'adresse IP* (valeur par défaut) : Une adresse IP dynamique est attribuée à votre appareil. • *Statique* : Vous saisissez une adresse IP statique.
Route par défaut	Indiquez si la route vers ce partenaire de communication doit être définie comme route par défaut. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Création entrée NAT	Indiquez si le NAT (Network Address Translation) doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Adresse IP locale	Uniquement si **Mode Adresse IP** = *Statique*

Champ	Description
	Saisissez l'adresse IP statique du partenaire de communication.
Entrées de route	Uniquement si **Mode Adresse IP** = *Statique* Définissez d'autres entrées de routage pour ce partenaire de communication. Ajoutez de nouvelles entrées à l'aide de l'option **Ajouter**. • *Adresse IP distante* : adresse IP de l'hôte ou du réseau de destination. • *Masque réseau* : masque de réseau pour **Adresse IP distante**. En l'absence de saisie, votre appareil utilise un masque de réseau par défaut. • *Métrique* : plus la valeur est faible, plus la priorité de la route est élevée (plage de valeurs *0*... *15*). La valeur par défaut est *1*.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Bloquer après erreur de connexion pour	Saisissez le nombre de secondes durant lesquelles aucune nouvelle tentative ne doit être effectuée à l'aide de votre appareil après un échec de connexion. La valeur par défaut est *60*.
Nombre maximal de tentative de composition du numéro	Saisissez le nombre d'échecs de connexion après lequel l'interface est bloquée. Les valeurs possibles sont comprises entre *0* et *100*. La valeur par défaut est *5*.
Authentification	Sélectionnez le protocole d'authentification pour ce partenaire de communication. Sélectionnez l'authentification spécifiée par votre fournisseur. Valeurs possibles : • *PAP* (valeur par défaut) : Exécuter uniquement PAP (PPP Password Authentication Protocol), le mot de passe est transmis sans cryptage.

Champ	Description
	• *CHAP* : exécuter uniquement CHAP (PPP Challenge Handshake Authentication Protocol selon la RFC 1994), le mot de passe est transmis de façon cryptée. • *PAP/CHAP* : exécuter CHAP en priorité, sinon PAP. • *MS-CHAPv1* : exécuter uniquement MS-CHAP version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP* : exécuter CHAP en priorité, puis le protocole d'authentification exigé par le partenaire de communication en cas de rejet. (MSCHAP version 1 ou 2 possible.) • *MS-CHAPv2*: Exécuter uniquement MS-CHAP version 2. • *aucun*: Certains fournisseurs n'utilisent pas d'authentification. Si tel est le cas, sélectionnez cette option.
Négociation DNS	Indiquez si votre appareil reçoit des adresses IP pour **Serveur DNS primaire** et **Serveur DNS secondaire** du partenaire de communication ou s'il les envoie au partenaire de communication. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Priorétiser les paquets TCP ACK	Indiquez si le téléchargement TCP doit être optimisé en cas de chargement TCP intensif. Cette fonction est spécifiquement destinée aux bandes passantes asymétriques (ADSL). Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Contrôle d'accessibilité LCP	Indiquez si l'accessibilité du dispositif doit être contrôlée par l'envoi d'Echo requests ou d'Echo replies LCP. Il est ainsi possible, en cas de perturbation sur la ligne, de passer plus rapidement à une ligne de sauvegarde. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
MTU	Saisissez la taille maximale de paquet (Maximum Transfer

Champ	Description
	Unit, MTU) en octets pouvant être utilisée pour la connexion. Avec l'option par défaut *Automatique*, la valeur est définie par le protocole Link Control Protocol lors de l'établissement de la connexion. Si vous désactivez l'option *Automatique*, vous pouvez entrer une valeur. Les valeurs possibles sont comprises entre *1* et *8192*. La valeur par défaut est *0*.

12.1.2 PPTP

Le menu **WAN**->**Internet + composer**->**PPTP** affiche la liste de toutes les interfaces PPTP.

Ce menu permet de configurer une connexion Internet utilisant pour son établissement le protocole Point-to-Point Tunneling Protocol (PPTP). Cela est p. ex. nécessaire en Autriche.

12.1.2.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres interfaces PPTP.

Le menu **WAN**->**Internet + composer**->**PPTP**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez un nom pour désigner clairement la connexion Internet. Dans ce champ, le premier caractère ne peut pas être un chiffre. Les caractères spéciaux et trémas ne peuvent pas non plus être utilisés.
Interface Ethernet-PPTP	Sélectionnez l'interface IP utilisée pour le transport des paquets vers le dispositif PPTP. En cas d'utilisation d'un modem DSL externe, sélectionnez ici

Champ	Description
	le port Ethernet auquel le modem est raccordé. En cas d'utilisation du modem DSL interne, sélectionnez l'interface EthoA configurée pour cette connexion dans **Interfaces physiques**->**ATM**->**Profils**->**Nouveau**, p. ex. *ethoa50-0*.
Nom de l'utilisateur	Saisissez le nom d'utilisateur.
Mot de passe	Saisissez le mot de passe.
Toujours actif	Indiquez si l'interface doit être activée en permanence. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. N'activez cette option que si vous disposez d'un accès Internet avec un forfait fixe.
Timeout en cas d'inactivité	Uniquement si **Toujours actif** est désactivé. Saisissez l'intervalle d'inactivité en secondes. Vous définissez ainsi le nombre de secondes devant s'écouler entre l'envoi du dernier paquet de données et la déconnexion. Les valeurs possibles sont comprises entre *0* et *3600* (secondes). *0* permet de désactiver le Timeout. La valeur par défaut est *300*. Ex. *10* pour les transmissions FTP, *20* pour les transmissions de LAN à LAN, *90* pour les connexions Internet.

Champs du menu Mode IP et routes

Champ	Description
Mode Adresse IP	Indiquez si une adresse IP statique ou dynamique doit être affectée à votre appareil. Valeurs possibles : • *Appeler l'adresse IP* (valeur par défaut) : Une adresse IP à validité temporaire est attribuée de manière dynamique à votre appareil.

Champ	Description
	• *Statique* : Vous saisissez une adresse IP statique.
Route par défaut	Indiquez si la route vers ce partenaire de communication doit être définie comme route par défaut. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Création entrée NAT	Indiquez si le NAT (Network Address Translation) doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Adresse IP locale	Uniquement pour **Mode Adresse IP** = *Statique* Attribuez à l'interface PPTP une adresse IP de votre LAN à utiliser comme adresse source interne de votre appareil.
Entrées de route	Uniquement si **Mode Adresse IP** = *Statique* Définissez d'autres entrées de routage pour ce partenaire PPTP. Ajoutez de nouvelles entrées à l'aide de l'option **Ajouter**. • *Adresse IP distante* : adresse IP de l'hôte ou du réseau de destination. • *Masque réseau* : masque de réseau pour **Adresse IP distante**. En l'absence de saisie, votre appareil utilise un masque de réseau par défaut. • *Métrique* : plus la valeur est faible, plus la priorité de la route est élevée (plage de valeurs *0*... *15*). La valeur par défaut est *1*.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Bloquer après erreur de connexion pour	Saisissez le nombre de secondes durant lesquelles aucune nouvelle tentative ne doit être effectuée à l'aide de votre appa-

Champ	Description
	reil après un échec de connexion. La valeur par défaut est *60*.
Nombre maximal de tentative de composition du numéro	Saisissez le nombre d'échecs de connexion après lequel l'interface est bloquée. Les valeurs possibles sont comprises entre *0* et *100*. La valeur par défaut est *5*.
Authentification	Sélectionnez le protocole d'authentification pour cette connexion Internet. Sélectionnez l'authentification spécifiée par votre fournisseur. Valeurs possibles : • *PAP* (valeur par défaut) : Exécuter uniquement PAP (PPP Password Authentication Protocol), le mot de passe est transmis sans cryptage. • *CHAP* : exécuter uniquement CHAP (PPP Challenge Handshake Authentication Protocol selon la RFC 1994), le mot de passe est transmis de façon cryptée. • *PAP/CHAP* : exécuter CHAP en priorité, sinon PAP. • *MS-CHAPv1* : exécuter uniquement MS-CHAP version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP* : exécuter CHAP en priorité, puis le protocole d'authentification exigé par le partenaire de communication en cas de rejet. (MSCHAP version 1 ou 2 possible.) • *MS-CHAPv2*: Exécuter uniquement MS-CHAP version 2. • *aucun*: Certains fournisseurs n'utilisent pas d'authentification. Si tel est le cas, sélectionnez cette option.
Négociation DNS	Indiquez si votre appareil reçoit des adresses IP pour **Serveur DNS primaire** et **Serveur DNS secondaire** du partenaire de communication ou s'il les envoie au partenaire de communication. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Champ	Description
Priorétiser les paquets TCP ACK	Indiquez si le téléchargement TCP doit être optimisé en cas de chargement TCP intensif. Cette fonction est spécifiquement destinée aux bandes passantes asymétriques (ADSL). Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Mode adresse PPTP	Permet d'afficher le mode d'adresses. La valeur ne peut pas être modifiée. Valeurs possibles : • *Statique* : l'**Adresse PPTP-IP locale** est affectée au port Ethernet sélectionné.
Adresse PPTP-IP locale	Attribuez à l'interface PPTP une adresse IP utilisée comme adresse source. La valeur par défaut est *10.0.0.140*.
Adresse PPTP-IP distante	Saisissez l'adresse IP du partenaire PPTP. La valeur par défaut est *10.0.0.138*.
Contrôle d'accessibilité LCP	Indiquez si l'accessibilité du dispositif doit être contrôlée par l'envoi d'Echo requests ou d'Echo replies LCP. Il est ainsi possible, en cas de perturbation sur la ligne, de passer plus rapidement à une ligne de sauvegarde. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

12.1.3 RNIS

Le menu **WAN**->**Internet + composer**->**RNIS** affiche la liste de toutes les interfaces RNIS.

Ce menu permet de configurer les connexions RNIS suivantes :

- Accès Internet via RNIS
- Couplage de LAN à LAN via RNIS
- Remote (Mobile) Dial-in

- Utilisation de la fonction RNIS Callback

12.1.3.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres interfaces RNIS.

Le menu **WAN**->**Internet + composer**->**RNIS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez un nom pour désigner clairement le partenaire de communication. Dans ce champ, le premier caractère ne peut pas être un chiffre. Les caractères spéciaux et trémas ne peuvent pas non plus être utilisés.
Type de connexion	Sélectionnez le protocole Layer 1 devant être utilisé par votre appareil. Cette configuration s'applique aux connexions sortantes vers le partenaire de connexion et uniquement pour les connexions entrantes du partenaire de connexion lorsque celui-ci peut être identifié à l'aide du Calling Party Number. Valeurs possibles : • *RNIS 64 kbits/s* : pour des connexions de données RNIS 64 kbit/s • *RNIS 56 kbits/s* : pour des connexions de données RNIS 56 kbit/s
Nom de l'utilisateur	Indiquez le numéro d'identification de votre appareil (nom d'utilisateur PPP local).
Utilisateur distant (uniquement numérotation)	Indiquez le numéro d'identification du dispositif (nom d'utilisateur PPP distant).
Mot de passe	Saisissez le mot de passe.
Toujours actif	Indiquez si l'interface doit être activée en permanence.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. N'activez cette option que si vous disposez d'un accès Internet avec un forfait fixe.
Timeout en cas d'inactivité	Uniquement si **Toujours actif** est désactivé. Saisissez l'intervalle d'inactivité en secondes. Vous définissez ainsi le nombre de secondes devant s'écouler entre l'envoi du dernier paquet de données et la déconnexion. Valeurs possibles comprises entre *0* et *3600* (secondes). *0* permet de désactiver le Timeout. La valeur par défaut est *20*.

Champs du menu Mode IP et routes

Champ	Description
Mode Adresse IP	Indiquez si une adresse IP statique ou dynamique doit être affectée à votre appareil. Valeurs possibles : • *Statique* (valeur par défaut) : Vous entrez une adresse IP statique. • *Mettre à disposition l'adresse IP* : votre appareil attribue une adresse IP dynamique au dispositif. • *Appeler l'adresse IP* : une adresse IP dynamique est attribuée à votre appareil.
Route par défaut	Uniquement si **Mode Adresse IP** = *Statique* et *Appeler l'adresse IP* Indiquez si la route vers ce partenaire de communication doit être définie comme route par défaut. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Création entrée NAT	Uniquement si **Mode Adresse IP** = *Statique* et *Appeler*

Champ	Description
	l'adresse IP Lorsqu'une connexion Internet RNIS est configurée, indiquez si le NAT (Network Address Translation) doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Adresse IP locale	Uniquement si **Mode Adresse IP** = *Statique* Attribuez à l'interface RNIS l'adresse IP de votre LAN à utiliser comme adresse source interne de votre appareil.
Entrées de route	Uniquement si **Mode Adresse IP** = *Statique* Définissez d'autres entrées de routage pour ce partenaire de communication. • *Adresse IP distante* : adresse IP de l'hôte ou du réseau de destination. • *Masque réseau* : masque de réseau pour **Adresse IP distante**. En l'absence de saisie, votre appareil utilise un masque de réseau par défaut. • *Métrique* : plus la valeur est faible, plus la priorité de la route est élevée (plage de valeurs *0*... *15*). La valeur par défaut est *1*.
Pool d'affectation IP	Uniquement si **Mode Adresse IP** = *Mettre à disposition l'adresse IP* Sélectionnez un pool d'adresses IP configuré dans le menu **WAN**->**Internet + composer**->**Pool IP**. Si aucun pool d'adresses IP n'a encore été configuré, la mention *Pas encore défini* s'affiche dans ce champ.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Bloquer après erreur de connexion pour	Saisissez le nombre de secondes durant lesquelles aucune nouvelle tentative ne doit être effectuée à l'aide de votre appareil après un échec de connexion.

Champ	Description
	La valeur par défaut est *300*.
Nombre maximal de tentative de composition du numéro	Saisissez le nombre d'échecs de connexion après lequel l'interface est bloquée. Les valeurs possibles sont comprises entre *0* et *100*. La valeur par défaut est *5*.
Type d'utilisation	Choisissez, le cas échéant, une utilisation spéciale de l'interface. Valeurs possibles : • *Par défaut* (valeur par défaut) : aucun type particulier n'est défini. • *Uniquement numérotation* : l'interface est utilisée pour les communications téléphoniques entrantes et pour les Callbacks initiés de l'extérieur. • *Choix multiple (uniquement numérotation)* : l'interface est définie en tant que partenaire de communication Multi-User, ce qui signifie que plusieurs clients se connectent à l'aide du même nom d'utilisateur et du même mot de passe.
Authentification	Sélectionnez le protocole d'authentification pour ce partenaire PPTP. Valeurs possibles : • *PAP* (valeur par défaut) : Exécuter uniquement PAP (PPP Password Authentication Protocol), le mot de passe est transmis sans cryptage. • *CHAP* : exécuter uniquement CHAP (PPP Challenge Handshake Authentication Protocol selon la RFC 1994), le mot de passe est transmis de façon cryptée. • *PAP/CHAP* : exécuter CHAP en priorité, sinon PAP. • *MS-CHAPv1* : exécuter uniquement MS-CHAP version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP* : exécuter CHAP en priorité, puis le protocole d'authentification exigé par le partenaire de com-

Champ	Description
	munication en cas de rejet. (MSCHAP version 1 ou 2 possible.) • *MS-CHAPv2*: Exécuter uniquement MS-CHAP version 2. • *aucun*: Certains fournisseurs n'utilisent pas d'authentification. Si tel est le cas, sélectionnez cette option.
Cryptage	Uniquement pour **Authentification** = *MS-CHAPv2* Choisissez, le cas échéant, le type de cryptage à utiliser pour l'échange de données avec le partenaire de communication. Cela n'est possible que si la compression avec STAC ou MS-STAC n'est pas activée pour la connexion. Si l'option **Cryptage** est définie, le dispositif doit également être pris en charge pour qu'une connexion puisse être établie. Valeurs possibles : • *aucun* (valeur par défaut) : aucun cryptage MPP n'est utilisé. • *Activé* : le cryptage MPP V2 128 bits est utilisé conformément à la RFC 3078. • *Compatible Windows* : le cryptage MPP V2 128 bits est compatible avec Microsoft et Cisco.

Mode Callback	Sélectionnez la fonction Mode Callback.
	
	Valeurs possibles :
	• *aucun* (valeur par défaut) : votre appareil n'effectue aucun rappel.
	• *Actif* : sélectionnez l'une des options suivantes :
	  • *Pas de négociation PPP* : votre appareil appelle le partenaire de connexion pour demander un rappel.
	  • *Mode Windows client* : votre appareil appelle le partenaire de connexion pour demander un rappel via le protocole CBCP (Callback Control Protocol). Ce paramètre est nécessaire pour les clients Windows.
	• *Passif* : sélectionnez l'une des options suivantes :
	  • *Négociation PPP ou CLID* : votre appareil rappelle immédiatement lorsque le partenaire de communication l'y invite.
	  • *Mode serveur Windows* : votre appareil appelle après

Champ	Description
	un délai proposé par le client Microsoft (NT : 10 secondes, systèmes plus récents : 12 secondes). Avec le réglage **Mode** *Sortant* ou *Les deux*, il utilise le numéro d'appel (**Entrées**->**Numéro d'appel**) configuré pour le partenaire de communication. A défaut de numéro configuré, le numéro nécessaire peut être communiqué par l'appelant dans une négociation PPP. Pour des raisons de sécurité, il est recommandé d'éviter autant que possible l'utilisation de cette configuration. Son utilisation est actuellement inévitable pour la connexion de clients Microsoft mobiles via un réseau RDT. • *Délai, uniquement CLID* : votre appareil rappelle après environ quatre secondes lorsque le partenaire de communication l'y invite. Utile uniquement pour CLID. • *Mode serveur Windows, numéro d'appel en option* : identique à *Mode serveur Windows* avec une option d'annulation. Pour des raisons de sécurité, il est recommandé d'éviter cette configuration. Le client Microsoft a ici en plus la possibilité d'annuler le Callback et de conserver la connexion initiale à votre appareil sans Callback. Cela ne s'applique que dans l'éventualité où aucun numéro sortant fixe n'est configuré pour le partenaire de communication. Cela est obtenu en fermant la boîte de dialogue qui apparaît en appuyant sur **Annuler**.

Champs du menu Options pour largeur de bande sur demande

Champ	Description
Groupage des canaux	Indiquez si le groupage des canaux doit être utilisé pour les connexions RNIS, ainsi que le type de groupage. Votre appareil prend en charge le groupage dynamique et statique des canaux pour les communications téléphoniques. Lors de l'établissement d'une communication, seul un canal B est ouvert dans un premier temps. Le groupage dynamique des canaux signifie que l'appareil, au besoin, c'est-à-dire en cas de débits de données importants, ouvre des canaux B RNIS supplémentaires afin d'augmenter le débit. Si le flux de données diminue, les canaux B supplémentaires se ferment de nouveau. Avec le groupage statique des canaux, vous déterminez au préalable le nombre de canaux B à utiliser par votre appareil, indépendamment des débits de données transmises.

Champ	Description
	Valeurs possibles : • *aucun* (valeur par défaut) : aucun groupage des canaux, un seul canal B est en toute circonstance disponible pour les connexions. • *Statique* : groupage statique des canaux. • *Dynamique* : groupage dynamique des canaux.

Champ du menu Numéros à composer

Champ	Description
Entrées	Ajoutez d'autres entrées à l'aide de l'option **Ajouter**.

Les champs du menu Configuration des numéros à composer (s'affiche uniquement pour Entrées = Ajouter)

Champ	Description
Mode	Uniquement si **Entrées** = *Ajouter* Le Calling Party Number de l'appelant est comparé avec celui entré sous **Numéro d'appel**. Indiquez si le **Numéro d'appel** doit être utilisé pour les appels entrants ou sortants ou pour les deux. Valeurs possibles : • *Les deux* (valeur par défaut) : pour les appels entrants et sortants. • *Entrant* : pour les appels entrants, lorsque le partenaire de communication doit se connecter à votre appareil. • *Sortant* : pour les appels sortants, lorsque vous devez vous connecter au partenaire de communication. Le numéro de l'appelant d'un appel entrant (Calling Party Number) est comparé avec le numéro entré sous **Numéro d'appel**.
Numéro d'appel	Saisissez les numéros d'appel du partenaire de communication.
Nombre de ports utilisés	Indiquez le port à utiliser.

Champs du menu Options IP

Champ	Description
Mode OSPF	Indiquez si une propagation doit être réalisée sur les routes de l'interface et/ou si des paquets correspondant au protocole OSPF doivent être envoyés via l'interface, et de quelle manière. Valeurs possibles : • *Passif* (valeur par défaut) : OSPF n'est pas activé pour cette interface : aucune propagation n'est effectuée sur les routes associées à l'interface, et aucun paquet correspondant au protocole OSPF n'est envoyé. Les réseaux accessibles via ces interfaces sont toutefois pris en compte lors du calcul des informations de routage et propagés via des interfaces actives. • *Actif* : OSPF est activé pour cette interface : une propagation est effectuée sur les routes associées à l'interface et/ou des paquets correspondant au protocole OSPF sont envoyés. • *Inactif* : OSPF est désactivé pour cette interface.
Mode Proxy ARP	Indiquez si votre appareil doit répondre aux requêtes ARP-Request de son propre LAN à la place du partenaire de communication spécifique et, le cas échéant, de quelle façon. Valeurs possibles : • *Inactif* (valeur par défaut) : désactive Proxy-ARP pour ce partenaire de communication. • *Actif ou en veille* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au partenaire de connexion est *Actif* (activée) ou *En veille* (en veille). Si l'option *En veille* est sélectionnée, votre appareil répond uniquement à la requête ARP-Request ; la connexion s'établit uniquement lorsqu'une personne souhaite utiliser la route. • *Actif uniquement* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au partenaire de connexion est *Actif* (activée), c'est-à-dire lorsqu'une connexion au partenaire de connexion est déjà établie.
Négociation DNS	Indiquez si votre appareil reçoit des adresses IP pour **Serveur**

Champ	Description
	DNS primaire et **Serveur DNS secondaire** et **Serveur WINS Primaire** et **Secondaire** du partenaire de communication ou s'il les envoie au partenaire de communication. Sélectionnez `Activé` pour activer la fonction. La fonction est activée par défaut.

12.1.4 Pool IP

Dans le menu **Pool IP**, une liste de tous les pools IP est affichée.

Votre appareil peut faire fonction de serveur d'adresses IP dynamique pour les connexions PPP. Pour ce faire, mettez un ou plusieurs pools d'adresses IP à disposition. Ces adresses IP peuvent être attribuées à des partenaires de communication connectés pour la durée de la communication.

Les routes d'hôtes saisies ont toujours la priorité sur les adresses IP des pools d'adresses. Ainsi, lorsqu'un appel entrant a été authentifié, votre appareil vérifie d'abord si une route d'hôte a été saisie dans le tableau de routage pour l'appelant. Si tel n'est pas le cas, votre appareil peut attribuer une adresse IP issue d'un pool d'adresses (si disponible). Dans le cas de pools d'adresses contenant plusieurs adresses IP, vous ne pouvez pas déterminer les adresses à attribuer aux partenaires de communication. Les adresses sont d'abord simplement attribuées dans l'ordre indiqué. Lors d'une nouvelle tentative de connexion dans un intervalle d'une heure, le système tente de nouveau d'affecter l'adresse IP attribuée en dernier lieu à ce partenaire.

12.1.4.1 Editer ou Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres pools d'adresses IP. Sélectionnez le symbole pour traiter les entrées existantes.

Champs du menu Paramètres de base

Champ	Description
Nom de pool IP	Saisissez une description pour désigner clairement le pool d'adresses IP.
Plage d'adresses IP	Saisissez la première (premier champ) et la dernière (deuxième champ) adresse IP du pool d'adresses IP.
Serveur DNS	**Primaire** : saisissez l'adresse IP du serveur DNS qui doit être

Champ	Description
	utilisé de préférence par les clients qui reçoivent une adresse issue de ce pool d'adresses. **Secondaire** : saisissez l'adresse IP d'un autre serveur DNS.

12.2 Real Time Jitter Control

Pour les conversations téléphoniques via Internet, les paquets de données vocales ont normalement la plus haute priorité. Toutefois, en raison d'une faible bande passante de la connexion de chargement pendant une conversation téléphonique, des retards perceptibles peuvent être rencontrés pour la transmission vocale lorsque d'autres paquets de données sont acheminés simultanément.

La fonction Real Time Jitter Control apporte une solution à ce problème. Afin de ne pas bloquer la « ligne » trop longtemps pour les paquets de données vocales, la taille des autres paquets de données est réduite pendant une conversation téléphonique.

12.2.1 Interfaces régulées

Le menu **WAN**->**Real Time Jitter Control**->**Interfaces régulées** affiche la liste de toutes les interfaces pour lesquelles la fonction Real Time Jitter Control est configurée.

12.2.1.1 Nouveau

Sélectionnez le bouton **Nouveau** afin d'optimiser la transmission vocale pour d'autres interfaces.

Le menu **WAN**->**Real Time Jitter Control**->**Interfaces régulées**->**Nouveau** se compose des champs suivants :

Champs du menu Configuration de base

Champ	Description
Interface	Déterminez pour quelles interfaces la transmission vocale doit être optimisée.
Mode de contrôle	Sélectionnez le mode pour l'optimisation. Valeurs possibles : • *RTP-Stream contrôlés seulement* (valeur par défaut) : A l'aide des données acheminées par la passerelle Media

Champ	Description
	Gateway, le système reconnaît les échanges de données vocales et optimise la transmission vocale. • *Tous les RTP-Stream*: tous les flux RTP sont optimisés. • *Inactif*: l'optimisation de la transmission des données vocales n'est pas effectuée. • *Toujours* : l'optimisation de la transmission des données vocales est toujours effectuée.
Vitesse de chargement maximale	Saisissez la bande passante maximale disponible en chargement en kbits/s pour l'interface sélectionnée.

Chapitre 13 VPN

L'abréviation VPN (Virtual Private Network) désigne une connexion utilisant Internet comme « moyen de transport » mais n'étant pas accessible publiquement. Seuls les utilisateurs autorisés ont accès à un réseau de ce type, également appelé de manière illustrative tunnel VPN. Généralement, les données transportées via un VPN sont cryptées.

Un VPN permet p. ex. à un représentant commercial ou à un collaborateur travaillant à domicile d'accéder aux données du réseau d'entreprise. Les filiales peuvent également être connectées au siège par VPN.

Pour la mise en place d'un tunnel VPN, différents protocoles sont à votre disposition, tels qu'IPSec ou PPTP.

L'authentification des partenaires de communication s'effectue à l'aide d'un mot de passe, de Preshared Keys ou de certificats.

Pour IPSec, le cryptage des données est réalisé p. ex. à l'aide d'AES ou de 3DES ; pour PPTP, MPPE peut être utilisé.

13.1 IPSec

IPSec permet la mise en place de connexions sécurisées entre deux emplacements (VPN). Grâce à cela, des données d'entreprise sensibles peuvent également être transmises via un média à la sécurité limitée tel qu'Internet. Les appareils utilisés représentent dans ce cadre les extrémités du tunnel VPN. Pour l'IPSec, il s'agit d'une série de normes IETF (Internet Engineering Task Force), précisant les mécanismes de protection et d'authentification de paquets IP. IPSec propose des mécanismes permettant de crypter et décrypter les données transmises dans les paquets IP. De plus, l'implémentation IPSec peut être intégrée de manière transparente à une infrastructure de clés publiques (PKI, voir *Certificats* sur la page 43). L'implémentation IPSec atteint cet objectif d'une part par l'utilisation des protocoles Authentication Header (AH) et Encapsulated Security Payload (ESP). D'autre part, des mécanismes de gestion de clés cryptographiques tels que le protocole Internet Key Exchange (IKE) sont utilisés.

Filtres supplémentaires du trafic de données

Les passerelles **Gigaset** prennent en charge deux méthodes différentes pour établir des connexions IPSec :

- une méthode basée sur les directives et
- une méthode par routage.

La méthode basée sur les directives implique l'usage de filtres d'échange de données pour la négociation des IPSec-Phase-2-SAs. Ce mécanisme permet de filtrer très finement les paquets IP, jusqu'à l'échelle du protocole et du port.

La méthode par routage offre plusieurs avantages par rapport à la méthode basée sur les directives, notamment l'utilisation de NAT/PAT au sein d'un tunnel, la possibilité d'associer IPSec à des protocoles de routage et la réalisation de scénarios de sauvegarde VPN. Dans le cadre de la méthode par routage, les routes configurées ou apprises dynamiquement sont utilisées pour la négociation des IPSec-Phase-2-SAs. Cette méthode permet certes de simplifier de nombreuses configurations, mais elle peut également entraîner des problèmes liés à des routes entrant en conflit ou à un filtrage plus grossier des échanges de données.

La paramètre **Filtres supplémentaires du trafic de données** apporte une solution à ce problème. Il vous permet de procéder à un filtrage plus fin, en indiquant par exemple l'adresse IP source ou le port source. Si un **Filtres supplémentaires du trafic de données** est configuré, celui-ci est utilisé pour la négociation des IPSec-Phase-2-SAs. La route ne détermine alors que l'échange de données devant être acheminé.

Tout paquet IP non conforme au **Filtres supplémentaires du trafic de données** défini est rejeté.

Si un paquet IP respecte les exigences d'un **Filtres supplémentaires du trafic de données**, la négociation IPSec-Phase-2 commence et l'échange de données est transmis via le tunnel.

Note

La paramètre **Filtres supplémentaires du trafic de données** ne concerne que l'initiateur de la connexion IPSec, dans la mesure où il s'applique uniquement aux échanges de données sortants.

Note

Veillez à ce que la configuration des directives de phase 2 soit identique pour chacun des nœuds d'extrémité du tunnel IPSec.

13.1.1 IPSec-Peers

Le terme Peer désigne le nœud d'extrémité d'une communication dans un réseau informatique. Chaque Peer propose ses services et utilise ceux des autres Peers.

Dans le menu **VPN**->**IPSec**->**IPSec-Peers**, une liste de tous les Peers IPSec configurés est affichée.

Surveillance de Peers

L'accès au menu de surveillance d'un Peer s'effectue par la sélection du bouton du Peer correspondant dans la liste des Peers. Voir *Valeurs de la liste Tunnel IPSec* sur la page 428.

13.1.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres Peers IPSec.

Le menu **VPN**->**IPSec**->**IPSec-Peers**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres Peer

Champ	Description
État administratif	Sélectionnez l'état dans lequel vous souhaitez placer le Peer après l'enregistrement de la configuration du Peer. Valeurs possibles : • `Actif` (valeur par défaut) : le Peer peut directement être utilisé après l'enregistrement de la configuration pour la mise en place d'un tunnel. • `Inactif` : le Peer n'est dans un premier temps pas disponible après l'enregistrement de la configuration.
Description	Saisissez une description du Peer afin de l'identifier. L'entrée peut contenir 255 caractères maximum.
Adresse Peer	Saisissez l'adresse IP officielle du Peer ou son nom d'hôte résolvable. Cette saisie peut être ignorée dans certaines configurations, ce qui implique toutefois que votre appareil ne peut pas initier de connexion IPSec.
ID Peer	Sélectionnez le type d'ID et saisissez l'ID du Peer. Cette saisie peut être ignorée dans certaines configurations.

Champ	Description
	L'entrée peut contenir 255 caractères maximum. Types d'ID possibles : • *Fully Qualified Domain Name (FQDN)* • *Adresse e-mail* • *Adresse IPV4* • *ASN.1-DN (Distinguished Name)* • *ID de clé* : Chaîne de caractères quelconque Sur l'appareil de Peer, cet ID correspond au paramètre **Valeur ID locale**.
IKE (Internet Key Exchange)	Non disponible pour les appareils de la série **WIxxxxn**. Ces appareils ne prennent en charge qu'IKEv1. Sélectionnez la version du protocole Internet Key Exchange à utiliser. Valeurs possibles : • *IKEv1* (valeur par défaut) : version 1 du protocole Internet Key Exchange • *IKEv2* : version 2 du protocole Internet Key Exchange
Méthode d'authentification	Uniquement pour **IKE (Internet Key Exchange)** = *IKEv2* Sélectionnez une méthode d'authentification. Valeurs possibles : • *Preshared Keys* (valeur par défaut) : si vous n'utilisez pas de certificats pour l'authentification, vous pouvez sélectionner des Preshared Keys. Ces éléments sont définis dans le cadre de la configuration Peer, sous **IPSec-Peers**. La Preshared Key est le mot de passe commun. • *Signature RSA* : les calculs de clé de phase 1 sont authentifiés à l'aide de l'algorithme de cryptage RSA.
Type ID local	Uniquement pour **IKE (Internet Key Exchange)** = *IKEv2* Sélectionnez un type d'ID local. Types d'ID possibles :

Champ	Description
	• *Fully Qualified Domain Name (FQDN)* • *Adresse e-mail* • *Adresse IPV4* • *ASN.1-DN (Distinguished Name)* • *ID de clé* : Chaîne de caractères quelconque
ID locale	Uniquement pour **IKE (Internet Key Exchange)** = *IKEv2* Indiquez l'ID de votre appareil. Pour **Méthode d'authentification** = *Signature DSA* ou *Signature RSA*, l'option **Utiliser le nom de sujet du certificat** est affichée. Lorsque vous activez l'option **Utiliser le nom de sujet du certificat**, le premier nom alternatif sujet indiqué dans le certificat est utilisé ou, à défaut, le nom de sujet du certificat. Remarque : Dans le cas où vous utilisez des certificats à des fins d'identification et où votre certificat contient des noms alternatifs sujet (voir *Certificats* sur la page 43), gardez bien à l'esprit que votre appareil sélectionne par défaut le premier nom alternatif sujet. Assurez-vous que votre Peer et vous-même utilisez bien le même nom : il faut que l'ID local et l'ID Peer configuré pour vous par votre partenaire soient identiques.
Preshared Key	Saisissez le mot de passe associé au Peer. L'entrée peut contenir 50 caractères maximum. Tous les caractères sont admis, sauf *0x* au début de l'entrée.

Champs du menu Routes d'interfaces

Champ	Description
Attribution des adresses IP	Sélectionnez le mode de configuration de l'interface. Valeurs possibles : • *Statique* (valeur par défaut) : saisissez une adresse IP statique. • *Client en mode configuration IKE* : uniquement disponible pour IKEv1. Sélectionnez cette option lorsque

Champ	Description
	votre passerelle doit recevoir une adresse IP en tant que client IPSec du serveur. • *Serveur en mode configuration IKE* : sélectionnez cette option lorsque votre passerelle doit recevoir une adresse IP en tant que clients se connectant au serveur. Celle-ci est prélevée du **Pool d'affectation IP** sélectionné.
mode de configuration	Uniquement si **Attribution des adresses IP** = *Serveur en mode configuration IKE* ou *Client en mode configuration IKE* Valeurs possibles : • *Pull* (valeur par défaut) : le client demande l'adresse IP et la passerelle répond à cette demande. • *Push* : la passerelle propose au client une adresse IP et le client doit l'accepter ou la rejeter. Cette valeur doit être identique pour les deux côtés du tunnel.
Pool d'affectation IP	Uniquement si **Attribution des adresses IP** = *Serveur en mode configuration IKE* Sélectionnez un pool d'adresses IP configuré dans le menu **VPN**->**IPSec**->**Pool IP**. Si aucun pool d'adresses IP n'a encore été configuré, la mention *Pas encore défini* s'affiche dans ce champ.
Route par défaut	Uniquement pour **Attribution des adresses IP** = *Statique* ou *Client en mode configuration IKE* Indiquez si la route vers ce Peer IPSec est définie comme route par défaut. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Adresse IP locale	Uniquement pour **Attribution des adresses IP** = *Statique* ou *Serveur en mode configuration IKE* Saisissez l'adresse WAN IP de votre connexion IPSec. Il peut s'agir de la même adresse IP que celle configurée en tant qu'adresse LAN IP dans votre routeur.

Champ	Description
Métrique	Uniquement pour **Attribution des adresses IP** = *Statique* ou *Client en mode configuration IKE* et **Route par défaut** = *Activé* Sélectionnez la priorité de la route. Plus la valeur que vous définissez est basse, plus la priorité de la route est élevée. Plage de valeurs de *0* à *15*. La valeur par défaut est *1*.
Entrées de route	Uniquement pour **Attribution des adresses IP** = *Statique* ou *Client en mode configuration IKE* Définissez des entrées de routage pour ce partenaire de communication. • *Adresse IP distante* : adresse IP de l'hôte ou des LAN de destination. • *Masque réseau* : masque de réseau pour l' *adresse IP distante*. • *Métrique* : plus faible est la valeur, plus élevée est la priorité de la route (plage de valeurs *0 - 15*). La valeur par défaut est *1*.

Champs du menu Filtres supplémentaires du trafic de données

Champ	Description
Filtres supplémentaires du trafic de données	Uniquement pour **IKE (Internet Key Exchange)** = *IKEv1* Créez un nouveau filtre à l'aide de l'option **Ajouter**.

Filtre supplémentaire de l'échange de données

Les passerelles **Gigaset** prennent en charge deux méthodes différentes pour établir des connexions IPSec :

- une méthode basée sur les directives et
- une méthode par routage.

La méthode basée sur les directives implique l'usage de filtres d'échange de données pour la négociation des IPSec-Phase-2-SAs. Ce mécanisme permet de filtrer très finement les paquets IP, jusqu'à l'échelle du protocole et du port.

La méthode par routage offre plusieurs avantages par rapport à la méthode basée sur les directives, notamment l'utilisation de NAT/PAT au sein d'un tunnel, la possibilité d'associer IPSec à des protocoles de routage et la réalisation de scénarios de sauvegarde VPN. Dans le cadre de la méthode par routage, les routes configurées ou apprises dynamiquement sont utilisées pour la négociation des IPSec-Phase-2-SAs. Cette méthode permet certes de simplifier de nombreuses configurations, mais elle peut également entraîner des problèmes liés à des routes entrant en conflit ou à un filtrage plus grossier des échanges de données.

La paramètre **Filtres supplémentaires du trafic de données** apporte une solution à ce problème. Il vous permet de procéder à un filtrage plus fin, en indiquant par exemple l'adresse IP source ou le port source. Si un **Filtres supplémentaires du trafic de données** est configuré, celui-ci est utilisé pour la négociation des IPSec-Phase-2-SAs. La route ne détermine alors que l'échange de données devant être acheminé.

Tout paquet IP non conforme au **Filtres supplémentaires du trafic de données** défini est rejeté.

Si un paquet IP respecte les exigences d'un **Filtres supplémentaires du trafic de données**, la négociation IPSec-Phase-2 commence et l'échange de données est transmis via le tunnel.

Note

La paramètre **Filtres supplémentaires du trafic de données** ne concerne que l'initiateur de la connexion IPSec, dans la mesure où il s'applique uniquement aux échanges de données sortants.

Note

Veillez à ce que la configuration des directives de phase 2 soit identique pour chacun des nœuds d'extrémité du tunnel IPSec.

Ajoutez d'autres filtres à l'aide de l'option **Ajouter**.

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une désignation pour le filtre.
Journal	Sélectionnez un protocole. L'option *Quelconque* (valeur par

Champ	Description
	défaut) convient à tous les protocoles.
Adresse IP source/ Masque de réseau	Définissez, si vous le souhaitez, les adresses IP source et le masque de réseau des paquets de données. Valeurs possibles : • *Quelconque* • *Hôte* : saisissez l'adresse IP de l'hôte. • *Réseau* (valeur par défaut) : saisissez les adresses de réseau et le masque de réseau correspondant.
Port source	Uniquement pour **Journal** = *TCP* ou *UDP* Saisissez le port source des paquets de données. Le paramètre par défaut *-Tous-* (= -1) signifie que le port n'est pas spécifié de manière plus détaillée.
Adresse IP de destination/Masque de réseau	Saisissez les adresses IP de destination, ainsi que le masque de réseau correspondant des paquets de données.
Port de destination	Uniquement pour **Journal** = *TCP* ou *UDP* Saisissez le port de destination des paquets de données. Le paramètre par défaut *-Tous-* (= -1) signifie que le port n'est pas spécifié de manière plus détaillée.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Options IPSec étendues

Champ	Description
Profil Phase-1	Sélectionnez un profil pour la phase 1. Outre les profils personnalisés, vous pouvez également utiliser des profils préconfigurés. Valeurs possibles : • *Aucun (utiliser le profil par défaut)* : permet d'utiliser le profil désigné comme profil par défaut sous **VPN->IPSec->Profils Phase-1**. • *Plusieurs propositions* : permet d'utiliser un profil spécial, contenant pour la phase 1 les propositions 3DES/MD5, AES/MD5 et Blowfish/MD5, nonobstant le choix de proposi-

Champ	Description
	tions du menu **VPN**->**IPSec**->**Profils Phase-1**. • *<Nom du profil>* : Permet d'utiliser un profil configuré pour la phase 1 dans le menu **VPN**->**IPSec**->**Profils Phase-1**.
Profil Phase-2	Sélectionnez un profil pour la phase 2. Outre les profils personnalisés, vous pouvez également utiliser des profils préconfigurés. Valeurs possibles : • *Aucun (utiliser le profil par défaut)* : permet d'utiliser le profil désigné comme profil par défaut sous **VPN**->**IPSec**->**Profils Phase-2**. • **Plusieurs propositions* : permet d'utiliser un profil spécial, contenant pour la phase 2 les propositions 3DES/MD5, AES-128/MD5 et Blowfish/MD5, nonobstant le choix de propositions du menu **VPN**->**IPSec**->**Profils Phase-2**. • *<Nom du profil>* : Permet d'utiliser un profil configuré pour la phase 2 dans le menu **VPN**->**IPSec**->**Profils Phase-2**.
Profil XAUTH	Sélectionnez un profil dans **VPN**->**IPSec**->**Profils XAUTH**, si vous souhaitez utiliser XAuth pour l'authentification de ce Peer IPSec. Lorsque XAuth est utilisé en mode configuration IKE, les transactions concernant XAuth sont traitées en premier, puis celles concernant le mode configuration IKE.
Nombre de connexions autorisées	Sélectionnez le nombre d'utilisateurs pouvant se connecter avec ce profil Peer. Valeurs possibles : • *Un utilisateur* (valeur par défaut) : un seul Peer peut se connecter aux données définies dans ce profil. • *Utilisateurs multiples* : plusieurs Peers peuvent se connecter aux données définies dans ce profil. A chaque demande de connexion aux données définies dans ce profil, l'entrée Peer est dupliquée.

Champ	Description
Mode démarrage	Sélectionnez la manière dont le Peer doit être activé. Valeurs possibles : • *Sur demande* (valeur par défaut) : le Peer est activé par un Trigger. • *Toujours actif* : le Peer est toujours activé.

Champs du menu Options IP étendues

Champ	Description
Interface publique	Définissez l'interface publique (ou WAN) via laquelle ce Peer doit se connecter avec son partenaire VPN. Si vous sélectionnez l'option *Choisi par le routage*, l'interface par laquelle l'échange de données s'effectue est définie par le tableau actuel de routage. Si vous sélectionnez une interface, celle-ci sera utilisée conformément au réglage dans **Mode Interface publique**.
Mode Interface publique	Déterminez le traitement du réglage dans **Interface publique**. Valeurs possibles : • *Forcer* : seule l'interface sélectionnée est utilisée indépendamment des priorités du tableau actuel de routage. • *Préféré* : l'interface sélectionnée est utilisée en fonction des priorités du tableau actuel de routage lorsqu'aucune route plus intéressante via une autre interface n'est disponible.
Adresse IP source publique	Si vous exploitez plusieurs connexions Internet en parallèle, vous pouvez indiquer ici l'adresse IP publique à utiliser pour l'échange de données du Peer en tant qu'adresse source. Indiquez si l'**Adresse IP source publique** doit être activée. Sélectionnez *Activé* pour activer la fonction. Saisissez dans la zone de texte l'adresse IP publique à utiliser comme adresse d'expédition. La fonction est désactivée par défaut.
Vérification de la route de retour	Indiquez si une vérification de la route de retour doit être activée pour l'interface vers le partenaire de communication. Sélectionnez *Activé* pour activer la fonction.

Champ	Description
	La fonction est désactivée par défaut.
MobIKE	Uniquement pour les Peers avec IKEv2. **MobIKE** permet d'actualiser uniquement ces adresses dans les SAs en cas d'adresses IP publiques variables, sans devoir renégocier les SAs elles-mêmes. La fonction est activée par défaut. Notez que MobIKE nécessite un client IPSec actuel, tel que le client actuel Windows 7 ou Windows 8 ou la dernière version du client IPSec bintec elmeg.
Proxy ARP	Indiquez si votre appareil doit répondre aux requêtes ARP-Request de son propre LAN à la place du partenaire de communication spécifique. Valeurs possibles : • *Inactif* (valeur par défaut) : désactive Proxy-ARP pour ce Peer IPSec. • *Actif ou en veille* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au Peer IPSec est *Actif* (activée) ou *En veille* (en veille). Si l'option *En veille* est sélectionnée, votre appareil répond uniquement à la requête ARP-Request ; la connexion s'établit uniquement lorsqu'une personne souhaite utiliser la route. • *Actif uniquement* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au Peer IPSec est *Actif* (activée), c'est-à-dire lorsqu'une connexion au Peer IPSec est déjà établie.

IPSec-Callback

Afin d'offrir une connexion sécurisée par Internet aux hôtes ne disposant pas d'une adresse IP fixe, les appareils **Gigaset** prennent en charge le service DynDNS. Ce service permet l'identification d'un Peer à l'aide d'un nom d'hôte résolvable par DNS. La configuration de l'adresse IP du Peer n'est pas nécessaire.

Le service DynDNS n'indique cependant pas si un Peer est réellement en ligne et ne peut pas inciter un Peer à établir une connexion Internet afin de permettre la création d'un tun-

nel IPSec via Internet. L'option IPSec-Callback offre cette possibilité : un appel RNIS direct auprès d'un Peer signale à ce dernier la mise en ligne et l'attente de l'établissement d'un tunnel IPSec via Internet. Si le Peer appelé ne dispose actuellement d'aucune connexion à Internet, il est incité par l'appel RNIS à en établir une. Cet appel RNIS ne génère (en fonction du pays d'utilisation) aucun coût, puisque l'appel RNIS ne doit pas être pris par votre appareil. L'identification de l'appelant à l'aide de son numéro d'appel RNIS suffit à initier la mise en place d'un tunnel.

Le réglage de ce service nécessite tout d'abord la configuration d'un numéro d'appel pour l'option IPSec-Callback dans la fenêtre passive du menu **Interfaces physiques**->**Ports RNIS**->**Configuration MSN**->**Nouveau**. Pour ce faire, vous pouvez utiliser la valeur *IPSec* pour le champ **Service**. Cette entrée veille à ce que les appels entrants sur ce numéro soient transmis au service IPSec.

Avec l'option Callback actif, dès qu'un tunnel IPSec est requis, le Peer est incité par un appel RNIS à en initier l'établissement. Avec l'option Callback passif, la création d'un tunnel est toujours initiée auprès du Peer lorsqu'un appel RNIS est reçu sur le numéro correspondant (**MSN** dans le menu **Interfaces physiques**->**Ports RNIS**->**Configuration MSN**->**Nouveau** pour le paramètre **Service** *IPSec*). Cela permet de garantir que les deux Peers sont joignables et que la connexion via Internet peut être établie. Aucun Callback n'est effectué lorsque des SAs (Security Associations) sont déjà présentes et donc que le tunnel vers le Peer existe déjà.

Note

Lorsqu'un tunnel vers un Peer doit être établi, le démon IPSec active tout d'abord l'interface par laquelle le tunnel doit être réalisé. Dans la mesure où IPSec est configuré sur l'appareil local avec DynDNS, une propagation est effectuée sur la propre adresse IP avant l'appel RNIS de l'appareil distant. Cela permet de garantir que l'appareil distant peut effectivement joindre l'appareil local au moment de l'initiation de la création du tunnel.

Transmission de l'adresse IP via RNIS

La transmission de l'adresse IP d'un appareil via RNIS (sur le canal D ou B) offre de nouvelles possibilités de configuration de VPN IPSec. Des restrictions, rencontrées dans la configuration IPSec avec des adresses IP dynamiques, peuvent de la sorte être contournées.

Note

Afin de pouvoir utiliser la fonction de transmission de l'adresse IP via RNIS, vous devez acquérir une licence complémentaire gratuite.

Pour obtenir les données des licences complémentaires, rendez-vous sur les pages d'octroi de licences en ligne dans la zone de support à l'adresse *www.bintec-elmeg.com*. Suivez les instructions d'octroi de licences en ligne.

Dans les versions du logiciel système antérieures à 7.1.4, l'IPSec RNIS Callback ne prenait en charge l'établissement d'un tunnel que lorsque l'adresse IP actuelle du déclencheur pouvait être déterminée de manière indirecte (p. ex. via DynDNS). DynDNS présente toutefois de lourds inconvénients, tels que le temps de latence avant l'actualisation effective de l'adresse IP dans la base de données. Cela peut avoir pour conséquence la propagation d'une adresse IP incorrecte via DynDNS. Ce problème est contourné par la transmission de l'adresse IP via RNIS. De plus, ce type de transmission d'adresses IP dynamiques permet l'utilisation du mode ID Protect sûr (mode principal) pour la création du tunnel.

Fonctionnement : différents modes sont disponibles pour la transmission de son adresse IP propre au Peer. L'adresse peut être transmise gratuitement sur le canal D ou B, l'appel du dispositif doit cependant être accepté, ce qui génère des coûts. Lorsqu'un Peer, dont l'adresse a été attribuée de manière dynamique, veut en inciter un autre à établir un tunnel IPSec, il peut transmettre sa propre adresse IP conformément aux réglages décrits dans *Champs du menu IPSec-Callback* sur la page 289. Tous les modes de transmission ne sont pas pris en charge par tous les opérateurs de télécommunications. En cas de doute, la sélection automatique par l'appareil permet de garantir l'utilisation de toutes les possibilités disponibles.

Note

Afin que votre appareil puisse identifier les informations du Peer appelé par l'adresse IP, la configuration de l'option Callback doit être effectuée de manière analogue sur les appareils concernés.

Les répartitions de rôles suivantes sont possibles :

- Une partie joue le rôle actif, l'autre le rôle passif.
- Les deux parties peuvent jouer les deux rôles (les deux).

La transmission de l'adresse IP et le début de la négociation IKE-Phase-1 se déroulent de

la manière suivante :

(1) Le Peer A (déclencheur du Callback) établit une connexion à Internet afin de se voir attribuer une adresse IP dynamique et d'être joignable par le Peer B via Internet.

(2) Votre appareil crée un jeton à durée de validité limitée et l'enregistre avec l'adresse IP actuelle dans l'entrée MIB appartenant au Peer B.

(3) Votre appareil effectue l'appel RNIS initial du Peer B. Ce faisant, l'adresse IP du Peer A ainsi que le jeton sont transmis conformément à la configuration de l'option Callback.

(4) Le Peer B extrait l'adresse IP du Peer A ainsi que le jeton de l'appel RNIS et les attribue au Peer A sur la base du Calling Party Number configuré (le numéro RNIS utilisé par le Peer A pour l'appel initial du Peer B).

(5) Le démon IPSec du Peer B sur votre appareil peut utiliser l'adresse IP transmise pour initier une négociation Phase-1 avec le Peer A. Ce faisant, le jeton est renvoyé dans une partie du payload au sein de la négociation IKE au Peer A.

(6) Le Peer A est désormais en mesure de comparer le jeton renvoyé par le Peer B avec les entrées dans le MIB et ainsi d'identifier le Peer, même sans connaître son adresse IP.

Le Peer A et le Peer B pouvant s'identifier mutuellement, des négociations à l'aide de Pre-shared Keys peuvent également être menées en mode ID Protect.

Note

Dans certains pays (p. ex. en Suisse), l'appel sur le canal D peut également engendrer des frais. Une mauvaise configuration de la partie appelée peut avoir pour conséquence l'ouverture du canal B par la partie appelée, ce qui crée des coûts pour la partie appelante.

Les options suivantes sont disponibles uniquement sur les appareils disposant d'une connexion RNIS :

Champs du menu IPSec-Callback

Champ	Description
Mode	Sélectionnez le mode Callback. Valeurs possibles : • *Inactif* (valeur par défaut) : IPSec-Callback est désactivé. L'appareil local ne réagit pas aux appels RNIS entrants et n'initie pas d'appels RNIS vers l'appareil distant.

Champ	Description
	• *Passif* : l'appareil local réagit uniquement aux appels RNIS entrants et initie le cas échéant l'établissement d'un tunnel IPSec vers le Peer. Aucun appel RNIS n'est effectué vers l'appareil distant pour l'inciter à la création d'un tunnel IPSec. • *Actif* : l'appareil local effectue un appel RNIS vers l'appareil distant pour l'inciter à la création d'un tunnel IPSec. L'appareil ne réagit pas aux appels RNIS entrants. • *Les deux* : votre appareil peut réagir aux appels RNIS entrants et effectuer un appel RNIS vers l'appareil distant. L'établissement d'un tunnel IPSec peut aussi bien être effectué (après un appel RNIS entrant) qu'incité (par un appel RNIS sortant).
Numéro d'appel entrant	Uniquement pour **Mode** = *Passif* ou *Les deux* Indiquez le numéro RNIS à partir duquel l'appareil distant appelle l'appareil local (Calling Party Number). Vous pouvez également utiliser des caractères génériques.
Numéro d'appel sortant	Uniquement pour **Mode** = *Actif* ou *Les deux* Indiquez le numéro RNIS sous lequel l'appareil local appelle l'appareil distant (Called Party Number). Vous pouvez également utiliser des caractères génériques.
Transmettre l'adresse IP propre par RNIS/ GSM	Indiquez si l'adresse IP de l'appareil propre doit être transmise par RNIS pour l'IPSec-Callback. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Mode de transmission	Uniquement pour **Transmettre l'adresse IP propre par RNIS/ GSM** = activé Indiquez dans quel mode votre appareil doit essayer de transmettre son adresse IP au Peer. Valeurs possibles : • *Détection automatique du meilleur mode* : votre appareil détermine automatiquement le mode approprié. Avec ce réglage, tous les modes du canal D sont essayés avant l'utilisation du canal B. (L'utilisation du canal B génère

Champ	Description
	des coûts.) • *Détecter automatiquement les modes de canal D seulement* : votre appareil détermine automatiquement le mode du canal D approprié. L'utilisation du canal B est exclue. • *Utiliser le mode canal D spécifique* : votre appareil tente de transmettre l'adresse IP selon le mode défini dans le champ **Mode**. • *Le mode canal D spécifique essaie de revenir sur le canal B* : votre appareil tente de transmettre l'adresse IP selon le mode défini dans le champ **Mode**. En cas d'échec, l'adresse IP est transmise sur le canal B. (Cela génère des coûts.) • *Utiliser uniquement le mode canal B* : votre appareil transmet l'adresse IP sur le canal B. Cela génère des coûts.
Mode du canal D	Uniquement pour **Mode de transmission** = *Utiliser le mode canal D spécifique* ou *Le mode canal D spécifique essaie de revenir sur le canal B* Indiquez dans quel mode du canal D votre appareil doit essayer de transmettre l'adresse IP. Valeurs possibles : • *LLC* (valeur par défaut) : l'adresse IP est transmise dans les « LLC Information Elements » du canal D. • *SUBADDR* : l'adresse IP est transmise dans les « Subaddress Information Elements » du canal D. • *LLC et SUBADDR* : l'adresse IP est aussi bien transmise dans les « LLC Information Elements » que dans les « Subaddress Information Elements ».

13.1.2 Profils Phase-1

Dans le menu **VPN**->**IPSec**->**Profils Phase-1**, une liste de tous les profils IPSec-Phase-1 configurés est affichée.

Dans la colonne **Par défaut**, vous pouvez sélectionner le profil à utiliser comme profil par

défaut.

13.1.2.1 Nouveau

Sélectionnez le bouton **Nouveau** (dans **Créer un nouveau profil IKEv1** ou **Créer un nouveau profil IKEv2**) pour configurer d'autres profils.

Le menu **VPN**->**IPSec**->**Profils Phase-1**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètre Phase-1 (IKE) / Paramètre Phase-1 (IKEv2)

Champ	Description
Description	Saisissez une description permettant d'identifier clairement le type de règle.
Proposals	Dans ce champ, vous pouvez sélectionner toute combinaison d'algorithmes de cryptage et de hachage d'informations pour IKE-Phase-1 sur votre appareil. La combinaison de six algorithmes de cryptage et de quatre algorithmes de hachage d'informations donne 24 valeurs possibles dans ce champ. Au moins une proposition doit être présente. C'est pourquoi la première ligne du tableau ne peut pas être désactivée. Algorithmes de cryptage (**Cryptage**) : • *3DES* (valeur par défaut) : 3DES est une extension de l'algorithme DES présentant une longueur de clé effective de 112 bits, et qui est donc considéré comme sûr. Il s'agit de l'algorithme le plus lent pris en charge à ce jour. • *Twofish* : Twofish était l'un des finalistes du concours AES (Advanced Encryption Standard). Cet algorithme est considéré comme aussi sûr que Rijndael (AES), mais est plus lent. • *Blowfish* : Blowfish est un algorithme à la fois très sûr et rapide. Twofish peut être considéré comme le successeur de Blowfish. • *CAST* : CAST est également un algorithme très sûr, un peu plus lent que Blowfish, mais plus rapide que 3DES. • *DES* : DES est un algorithme de cryptage assez ancien, qui est considéré comme peu sûr en raison de sa longueur de clé effective de 56 bits seulement. • *AES* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible

Champ	Description
	consommation de mémoire, résistance élevée aux attaques et rapidité générale. Avec cet algorithme, la longueur de clé AES du partenaire est utilisée. Si celui-ci a également sélectionné le paramètre *AES*, la longueur de clé utilisée est 128 bits. • *AES-128* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Dans ce cas, l'algorithme est utilisé avec une longueur de clé de 128 bits. • *AES-192* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Dans ce cas, l'algorithme est utilisé avec une longueur de clé de 192 bits. • *AES-256* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Dans ce cas, l'algorithme est utilisé avec une longueur de clé de 256 bits. Algorithmes de hachage (**Authentification**) : • *MD5* (valeur par défaut) : MD5 (Message Digest 5) est une fonction de hachage plutôt ancienne. Elle est utilisée pour IPSec avec une longueur de condensation de 96 bits. • *SHA1* : SHA 1 (Secure Hash Algorithmus 1) est une fonction de hachage conçue par la NSA (United States National Security Association). Elle est considérée comme sûre, mais est plus lente que MD5. Elle est utilisée pour IPSec avec une longueur de condensation de 96 bits. • *RipeMD 160* : RipeMD 160 est une fonction de hachage de 160 bits. Elle est utilisée en tant que remplacement sûr des fonctions MD5 et RipeMD. • *Tiger192* : Tiger 192 est une fonction relativement nouvelle et très rapide. Notez que la description du cryptage et de l'authentification ou des fonctions de hachage se base sur les connaissances et l'avis de l'auteur au moment de la rédaction de ce manuel. La qualité des algorithmes en particulier relève d'un point de vue relatif et peut se modifier en raison de développements mathé-

Champ	Description
	matiques et cryptographiques.
Groupe DH	Uniquement pour **Paramètre Phase-1 (IKE)** Le groupe Diffie-Hellman définit l'ensemble de paramètres sur lequel se base le calcul de clés pendant la phase 1. « MODP », telle que prise en charge par les appareils **Gigaset**, signifie « exponentiation modulaire ». Valeurs possibles : • *1 (768 bits)* : lors du calcul de clés Diffie-Hellman, l'exponentiation modulaire est utilisée avec 768 bits afin de générer les informations de cryptage. • *2 (1024 bits)* : lors du calcul de clés Diffie-Hellman, l'exponentiation modulaire est utilisée avec 1024 bits afin de générer les informations de cryptage. • *5 (1536 bits)* : lors du calcul de clés Diffie-Hellman, l'exponentiation modulaire est utilisée avec 1536 bits afin de générer les informations de cryptage.
Durée de vie	Déterminez la durée de vie pour la clé de phase 1. Conformément à la RFC 2407, la valeur standard est de huit heures, ce qui signifie que la clé doit être renouvelée toutes les huit heures. Les options suivantes sont disponibles pour définir la **Durée de vie** : • Saisie en **Secondes** : Indiquez la durée de vie pour la clé de phase 1 en secondes. Vous pouvez choisir n'importe quel nombre entier compris entre 0 et 2 147 483 647. La valeur par défaut est *14400*. • Saisie en **koctets** : Indiquez la durée de vie pour la clé de phase 1 en tant que quantité des données traitées en Ko. Vous pouvez choisir n'importe quel nombre entier compris entre 0 et 2 147 483 647. La valeur par défaut est *0*. La valeur par défaut conformément à la RFC est utilisée lorsque *0* seconde et *0* Ko sont entrés. La valeur standard conformément à la RFC est utilisée lorsque *0* seconde et *0* Ko sont entrés.

Champ	Description
Méthode d'authentification	Uniquement pour **Paramètre Phase-1 (IKE)** Sélectionnez une méthode d'authentification. Valeurs possibles : • *Preshared Keys* (valeur par défaut) : si vous n'utilisez pas de certificats pour l'authentification, vous pouvez sélectionner des Preshared Keys. Ces éléments sont définis dans le cadre de la configuration Peer, sous **VPN**->**IPSec**->**IPSec-Peers**. La Preshared Key est le mot de passe commun. • *Signature DSA* : les calculs de clé de phase 1 sont authentifiés à l'aide de l'algorithme de cryptage DSA. • *Signature RSA* : les calculs de clé de phase 1 sont authentifiés à l'aide de l'algorithme de cryptage RSA. • *Cryptage RSA* : avec le cryptage RSA, les données utiles d'identification sont également cryptées en tant que mesure de sécurité supplémentaire.
Certificat local	Uniquement pour **Paramètre Phase-1 (IKE)** Uniquement pour **Méthode d'authentification** = *Signature DSA*, *Signature RSA* ou *Cryptage RSA* Ce champ vous permet de sélectionner l'un de vos propres certificats pour l'authentification. Il affiche le numéro d'index de ce certificat et le nom sous lequel il est enregistré. Ce champ s'affiche uniquement pour les paramètres d'authentification basés sur des certificats et indique qu'un certificat est absolument indispensable.
Mode	Uniquement pour **Paramètre Phase-1 (IKE)** Sélectionnez le mode Phase-1. Valeurs possibles : • *Agressif* (valeur par défaut) : le mode agressif est indispensable si un des Peers ne dispose pas d'adresse IP statique et que des Preshared Keys sont utilisées pour l'authentification. Il ne requiert que trois messages pour la mise en place d'un canal sûr. • *Main Modus (ID Protect)* : ce mode (également appelé

Champ	Description
	Main Mode) requiert six messages pour un calcul de clés Diffie-Hellman et donc pour la mise en place d'un canal sûr via lequel les IPSec-SAs sont négociées. Il nécessite que les deux Peers disposent d'adresses IP statiques si des Preshared Keys sont utilisées pour l'authentification. Indiquez en outre si seul le mode sélectionné peut être utilisé (**Strict**) ou si le Peer peut également proposer un autre mode.
Type ID local	Uniquement pour **Paramètre Phase-1 (IKE)** Sélectionnez un type d'ID local. Valeurs possibles : • *Fully Qualified Domain Name (FQDN)* • *Adresse e-mail* • *Adresse IPV4* • *ASN.1-DN (Distinguished Name)*
Valeur ID locale	Uniquement pour **Paramètre Phase-1 (IKE)** Indiquez l'ID de votre appareil. Pour **Méthode d'authentification** = *Signature DSA*, *Signature RSA* ou *Cryptage RSA*, l'option **Utiliser le nom de sujet du certificat** est affichée. Lorsque vous activez l'option **Utiliser le nom de sujet du certificat**, le premier nom alternatif sujet indiqué dans le certificat est utilisé ou, à défaut, le nom de sujet du certificat. Remarque : Dans le cas où vous utilisez des certificats à des fins d'identification et où votre certificat contient des noms alternatifs sujet (voir *Certificats* sur la page 43), gardez bien à l'esprit que votre appareil sélectionne par défaut le premier nom alternatif sujet. Assurez-vous que votre Peer et vous-même utilisez bien le même nom : il faut que l'ID local et l'ID Peer configuré pour vous par votre partenaire soient identiques.

Contrôle d'accessibilité

Dans la communication de deux Peers IPSec, il peut arriver que l'un des deux ne soit pas

joignable en raison p. ex. de problèmes de routage ou d'un redémarrage. Un tel problème ne peut toutefois être identifié qu'une fois la fin de la durée de vie de la connexion sécurisée atteinte. Dans l'intervalle, les paquets de données sont perdus. Pour éviter cela, il existe différents mécanismes de contrôle d'accessibilité. Dans le champ **Contrôle d'accessibilité**, indiquez si un mécanisme doit être utilisé pour le contrôle de l'accessibilité d'un Peer.

Deux mécanismes sont disponibles dans ce but : Heartbeats et Dead Peer Detection.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Contrôle d'accessibilité	Uniquement pour **Paramètre Phase-1 (IKE)** Sélectionnez la méthode de contrôle du fonctionnement de la connexion IPSec. Outre la procédure standard Dead Peer Detection (DPD), la procédure (propriétaire) Heartbeat est également implémentée. En fonction de la configuration, celle-ci envoie ou reçoit des signaux toutes les 5 secondes. En leur absence, la SA est considérée comme non valide et rejetée après 20 secondes. Valeurs possibles : • *Détection automatique* (valeur par défaut) : votre appareil reconnaît et utilise le mode pris en charge par le dispositif. • *Inactif* : votre appareil n'envoie et n'attend aucun message Heartbeat. Si vous utilisez des appareils d'un autre fabricant, choisissez cette option. • *Heartbeats (attendre uniquement)* : votre appareil attend un message Heartbeat d'un Peer, mais n'en envoie aucun. • *Heartbeats (envoyer uniquement)* : votre appareil n'attend aucun message Heartbeat d'un Peer, mais en envoie un. • *Heartbeats (envoyer &attendre)* : votre appareil attend un message Heartbeat d'un Peer et en envoie un. • *Dead Peer Detection* : utiliser DPD (Dead Peer Detection) conformément à la RFC 3706. Le mécanisme DPD utilise un protocole requête-réponse afin de vérifier

Champ	Description
	l'accessibilité du dispositif, et peut être configuré de manière indépendante de part et d'autre. Avec cette option, l'accessibilité du Peer n'est contrôlée que lorsque des données doivent effectivement lui être envoyées. • *Dead Peer Detection (Idle)* : utiliser DPD (Dead Peer Detection) conformément à la RFC 3706. Le mécanisme DPD utilise un protocole requête-réponse afin de vérifier l'accessibilité du dispositif, et peut être configuré de manière indépendante de part et d'autre. Avec cette option, le contrôle est effectué à intervalles réguliers, indépendamment de transferts de données prévus. Uniquement pour **Paramètre Phase-1 (IKEv2)** Activez ou désactivez le contrôle d'accessibilité. La fonction est activée par défaut.
Temps de blocage	Déterminez combien de temps un Peer est bloqué pour l'établissement d'un tunnel après l'échec d'un établissement de tunnel de phase 1. Seules les tentatives d'établissement initiées localement sont concernées. Les valeurs comprises entre *-1* et *86400* (secondes) sont disponibles, la valeur *-1* signifie l'utilisation de la valeur contenue dans le profil par défaut, la valeur *0*, que le Peer n'est bloqué dans aucun cas. La valeur par défaut est *30*.
NAT-Traversal	Le NAT-T (NAT-Traversal) permet l'ouverture d'un tunnel IPSec également par un ou plusieurs appareils sur lesquels le NAT (Network Address Translation) est activé. En l'absence du NAT-T, des problèmes d'incompatibilité peuvent surgir entre IPSec et NAT (voir RFC 3715, section 2). Ceux-ci empêchent principalement l'établissement d'un tunnel IPSec par un hôte au sein d'un LAN et situé derrière un appareil NAT vers un autre hôte ou appareil. Le NAT-T permet la création de tels tunnels sans conflit avec un appareil NAT, un NAT activé est automatiquement identifié par le démon IPSec et le NAT-T est utilisé. Uniquement pour les *profils IKEv1*

Champ	Description
	Valeurs possibles : • *Activé* (valeur par défaut) : le NAT-Traversal est activé. • *Désactivé* : le NAT-Traversal est désactivé. • *Forcer* : l'appareil se comporte toujours comme si le NAT était utilisé. Uniquement pour les *profils IKEv2* Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Certificats CA	Uniquement pour **Paramètre Phase-1 (IKE)** Uniquement pour **Méthode d'authentification** = *Signature DSA*, *Signature RSA* ou *Cryptage RSA* Si vous activez l'option **Accepter comme fiable les certificats CA suivants**, vous pouvez sélectionner jusqu'à trois certificats CA devant être acceptés pour ce profil. Cette option ne peut être configurée que si des certificats sont chargés.

13.1.3 Profils Phase-2

Tout comme pour la phase 1, vous pouvez définir des profils pour la phase 2 de l'établissement de tunnel.

Dans le menu **VPN**->**IPSec**->**Profils Phase-2**, une liste de tous les profils IPSec-Phase-2 configurés est affichée.

Dans la colonne **Par défaut**, vous pouvez sélectionner le profil à utiliser comme profil par défaut.

13.1.3.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres profils.

Le menu **VPN**->**IPSec**->**Profils Phase-2**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètre Phase-2 (IPSEC)

Champ	Description
Description	Saisissez une description permettant d'identifier clairement le profil. L'entrée peut contenir 255 caractères maximum.
Proposals	Dans ce champ, vous pouvez sélectionner toute combinaison d'algorithmes de cryptage et de hachage d'informations pour IKE-Phase-2 sur votre appareil. La combinaison de six algorithmes de cryptage et de deux algorithmes de hachage d'informations donne 12 valeurs possibles dans ce champ. Algorithmes de cryptage (**Cryptage**) : • *3DES* (valeur par défaut) : 3DES est une extension de l'algorithme DES présentant une longueur de clé effective de 112 bits, et qui est donc considéré comme sûr. Il s'agit de l'algorithme le plus lent pris en charge à ce jour. • *-- TOUS --* : toutes les options peuvent être utilisées. • *AES* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Avec cet algorithme, la longueur de clé AES du partenaire est utilisée. Si celui-ci a également sélectionné le paramètre *AES*, la longueur de clé utilisée est 128 bits. • *AES-128* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Dans ce cas, l'algorithme est utilisé avec une longueur de clé de 128 bits. • *AES-192* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Dans ce cas, l'algorithme est utilisé avec une longueur de clé de 192 bits. • *AES-256* : Rijndael a été choisi en tant que standard AES car il offre plusieurs avantages : création rapide de clés, faible consommation de mémoire, résistance élevée aux attaques et rapidité générale. Dans ce cas, l'algorithme est utilisé avec une longueur de clé de 256 bits. • *Twofish* : Twofish était l'un des finalistes du concours AES

Champ	Description
	(Advanced Encryption Standard). Cet algorithme est considéré comme aussi sûr que Rijndael (AES), mais est plus lent. • *Blowfish* : Blowfish est un algorithme à la fois très sûr et rapide. Twofish peut être considéré comme le successeur de Blowfish. • *CAST* : CAST est également un algorithme très sûr, un peu plus lent que Blowfish, mais plus rapide que 3DES. • *DES* : DES est un algorithme de cryptage assez ancien, qui est considéré comme peu sûr en raison de sa longueur de clé effective de 56 bits seulement. Algorithmes de hachage (**Authentification**) : • *MD5* (valeur par défaut) : MD5 (Message Digest 5) est une fonction de hachage plutôt ancienne. Elle est utilisée pour IPSec avec une longueur de condensation de 96 bits. • *-- TOUS --* : toutes les options peuvent être utilisées. • *SHA1* : SHA 1 (Secure Hash Algorithmus 1) est une fonction de hachage conçue par la NSA (United States National Security Association). Elle est considérée comme sûre, mais est plus lente que MD5. Elle est utilisée pour IPSec avec une longueur de condensation de 96 bits. Notez que RipeMD 160 et Tiger 192 ne sont pas disponibles pour le hachage d'informations dans la phase 2.
Utiliser groupe PFS	Le PFS (Perfect Forward Secrecy) requérant un calcul de clés Diffie-Hellman supplémentaire afin de générer de nouvelles informations de cryptage, vous devez sélectionner les caractéristiques de l'exponentiation. Si vous activez le PFS (*Activé*), les options sont les mêmes que pour la configuration de **Groupe DH** dans le menu **VPN**->**IPSec**->**Profils Phase-1**. Le PFS est utilisé pour protéger la clé d'une nouvelle Phase-2-SA, même si la clé de la Phase-1-SA est connue. Le champ présente les options suivantes : • *1 (768 bits)* : lors du calcul de clés Diffie-Hellman, l'exponentiation modulaire est utilisée avec 768 bits afin de générer les informations de cryptage. • *2 (1024 bits)* (valeur par défaut) : lors du calcul de clés

Champ	Description
	Diffie-Hellman, l'exponentiation modulaire est utilisée avec 1024 bits afin de générer les informations de cryptage. • *5 (1536 bits)* : lors du calcul de clés Diffie-Hellman, l'exponentiation modulaire est utilisée avec 1536 bits afin de générer les informations de cryptage.
Durée de vie	Définissez le mode de détermination de la durée de vie après l'expiration de laquelle les Phase-2-SAs doivent être renouvelées. Les nouvelles SAs sont déjà négociées peu avant l'expiration des SAs actuelles. Conformément à la RFC 2407, la valeur standard est de huit heures, ce qui signifie que la clé doit être renouvelée toutes les huit heures. Les options suivantes sont disponibles pour définir la **Durée de vie** : • Saisie en **Secondes** : Indiquez la durée de vie pour la clé de phase 2 en secondes. Vous pouvez choisir n'importe quel nombre entier compris entre *0* et *2147483647*. La valeur par défaut est *7200*. • Saisie en **koctets** : Indiquez la durée de vie pour la clé de phase 2 en tant que quantité des données traitées en Ko. Vous pouvez choisir n'importe quel nombre entier compris entre *0* et *2147483647*. La valeur par défaut est *0*. **Générer à nouveau la clé après** : déterminez à quel pourcentage de leur durée de vie les clés de la phase 2 sont renouvelées. Le pourcentage entré est appliqué tant sur la durée de vie en secondes que sur la durée de vie en Ko. La valeur par défaut est *80* %.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Compression IP	Indiquez si une compression doit être activée avant le cryptage des données. Pour les données facilement compressibles, cela peut permettre des performances plus élevées et des volumes

Champ	Description
	de données de transfert réduits. Cette option est déconseillée pour les connexions rapides ou les données non compressibles, les performances pouvant être fortement affectées par la charge de travail accrue due à la compression. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Contrôle d'accessibilité	Indiquez si des messages Heartbeats IPSec doivent être utilisés et, le cas échéant, de quelle façon. Afin de déterminer si une SA (Security Association) est encore valide, un Heartbeat IPSec **Gigaset** a été implémenté. En fonction de la configuration, celui-ci envoie ou reçoit des signaux toutes les 5 secondes. En leur absence, la SA est considérée comme non valide et rejetée après 20 secondes. Valeurs possibles : • *Détection automatique* (valeur par défaut) : reconnaît automatiquement si le dispositif est un appareil **Gigaset**. Dans ce cas, *Heartbeats (envoyer &attendre)* (dispositif avec **Gigaset**) ou *Inactif* (dispositif sans **Gigaset**) est défini. • *Inactif* : votre appareil n'envoie et n'attend aucun message Heartbeat. Si vous utilisez des appareils d'un autre fabricant, choisissez cette option. • *Heartbeats (attendre uniquement)* : votre appareil attend un message Heartbeat d'un Peer, mais n'en envoie aucun. • *Heartbeats (envoyer uniquement)* : votre appareil n'attend aucun message Heartbeat d'un Peer, mais en envoie un. • *Heartbeats (envoyer &attendre)* : votre appareil attend un message Heartbeat d'un Peer et en envoie un.
Propagation PMTU	Indiquez si durant la phase 2 la PMTU (Path Maximum Transfer Unit) doit être propagée. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

13.1.4 Profils XAUTH

Dans le menu **Profils XAUTH**, une liste de tous les profils XAuth est affichée.

La XAuth (Extended Authentication pour IPSec) est une méthode d'authentification supplémentaire pour les utilisateurs d'un tunnel IPSec.

En utilisant la XAuth, la passerelle peut jouer deux rôles différents, elle peut servir de serveur ou de client :

- La passerelle exige en tant que serveur des données d'identification.
- La passerelle fournit en tant que client ses données d'identification.

En mode serveur, plusieurs utilisateurs peuvent s'identifier à l'aide de XAuth, p. ex. des utilisateurs d'iPhones Apple. L'autorisation est contrôlée soit à l'aide d'une liste, soit via un serveur RADIUS. En cas d'utilisation d'un mot de passe unique (One Time Password, OTP), la vérification des mots de passe peut être prise en charge par un serveur de jetons (p. ex. avec le produit SecOVID de Kobil), installé derrière le serveur RADIUS. Si le siège d'une société est reliée à plusieurs filiales par IPSec, plusieurs Peers peuvent être configurés. En fonction de l'attribution de différents profils, un utilisateur spécifique peut utiliser le tunnel IPSec via différents Peers. Cela est par exemple utile lorsqu'un collaborateur travaille alternativement dans différentes filiales, chaque Peer représentant une filiale et le collaborateur souhaitant avoir accès au tunnel depuis chacune d'entre elles.

Après la conclusion réussie de l'IKE IPSec (phase 1) et avant le début de l'IKE (phase 2), la XAuth est exécutée.

Lorsque XAuth est utilisé en mode configuration IKE, les transactions concernant XAuth sont traitées en premier, puis celles concernant le mode configuration IKE.

13.1.4.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres profils.

Le menu **VPN**->**IPSec**->**Profils XAUTH**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description pour ce profil XAuth.
Rôle	Sélectionnez le rôle de la passerelle au cours de l'authentification XAuth.

Champ	Description
	Valeurs possibles : • *Serveur* (valeur par défaut) : la passerelle exige des données d'identification. • *Client* : la passerelle fournit ses données d'identification.
Mode	Uniquement pour **Rôle** = *Serveur* Sélectionnez la manière dont l'authentification est effectuée. Valeurs possibles : • *RADIUS* (valeur par défaut) : l'authentification est effectuée via un serveur RADIUS. Ce dernier est configuré dans le menu **Gestion du système**->**Authentification distante**->**RADIUS** et sélectionné dans le champ **ID groupe serveur RADIUS**. • *Local* : l'authentification est effectuée au moyen d'une liste locale.
Nom	Uniquement pour **Rôle** = *Client* Saisissez le nom d'authentification du client.
Mot de passe	Uniquement pour **Rôle** = *Client* Saisissez le mot de passe d'authentification.
ID groupe serveur RADIUS	Uniquement pour **Rôle** = *Serveur* Sélectionnez le groupe RADIUS configuré dans **Gestion du système**->**Authentification distante**->**RADIUS** souhaité.
Utilisateur	Uniquement pour **Rôle** = *Serveur* et **Mode** = *Local* Si votre passerelle est configurée en tant que serveur XAuth, les clients peuvent être identifiés au moyen d'une liste d'utilisateurs configurée localement. Définissez ici les membres du groupe d'utilisateurs de ce profil XAuth en saisissant le nom (**Nom**) et le mot de passe d'authentification du client (**Mot de passe**). Ajoutez des membres supplémentaires à l'aide du bouton **Ajouter**.

13.1.5 Pool IP

Dans le menu **Pool IP**, une liste de tous les pools IP pour vos connexions IPSec configurées est affichée.

Si vous avez configuré **Attribution des adresses IP** en tant que *Serveur en mode configuration IKE* pour un Peer IPSec, vous devez définir ici les pools IP à partir desquels les adresses IP sont attribuées.

13.1.5.1 Editer ou Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres pools d'adresses IP. Sélectionnez le symbole pour traiter les entrées existantes.

Champs du menu Paramètres de base

Champ	Description
Nom de pool IP	Saisissez une description pour désigner clairement le pool d'adresses IP.
Plage d'adresses IP	Saisissez la première (premier champ) et la dernière (deuxième champ) adresse IP du pool d'adresses IP.
Serveur DNS	**Primaire** : saisissez l'adresse IP du serveur DNS qui doit être utilisé de préférence par les clients qui reçoivent une adresse issue de ce pool d'adresses. **Secondaire** : saisissez l'adresse IP d'un autre serveur DNS.

13.1.6 Options

Le menu **VPN**->**IPSec**->**Options** se compose des champs suivants :

Champs du menu Options globales

Champ	Description
Activer IPSec	Indiquez si vous souhaitez activer IPSec. Sélectionnez *Activé* pour activer la fonction. Dès qu'un Peer IPSec est configuré, la fonction est activée.

Champ	Description
Supprimer la configuration IPSec complète	En cliquant sur le symbole , vous supprimez l'ensemble de la configuration IPSec de votre appareil. Cela annule tous les réglages effectués pendant la configuration IPSec. Une fois la configuration supprimée, vous pouvez recommencer avec une toute nouvelle configuration IPSec. La suppression de la configuration est uniquement possible lorsque l'option **Activer IPSec** n'est pas activée.
IPSec-Debug-Level	Sélectionnez la priorité des messages de journaux système du sous-système IPSec devant être enregistrés en interne. Valeurs possibles : • *Urgence* (priorité la plus haute) • *Alarme* • *Critique* • *Erreur* • *Avertissement !* • *Notification* • *Informations* • *Debug* (valeur par défaut, priorité la plus basse) Seuls les messages de journaux système présentant une priorité équivalente ou supérieure à celle indiquée sont enregistrés en interne, ce qui signifie qu'avec le niveau Syslog « Debug » tous les messages générés sont enregistrés.

Dans le menu **Paramètres étendus**, vous pouvez adapter certaines fonctions et caractéristiques aux besoins particuliers de votre environnement, ce qui signifie principalement que des marqueurs d'interopérabilité sont placés. Les valeurs par défaut sont mondialement valides et permettent à votre système de travailler sans problème avec d'autres appareils **Gigaset**, de sorte que vous ne devez modifier ces valeurs que si le dispositif est un produit tiers ou que vous savez qu'il nécessite des paramétrages spécifiques. Cela peut par exemple être le cas lorsque l'appareil distant utilise des implémentations IPSec plus anciennes.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
IPSec via TCP	Indiquez si IPSec via TCP doit être utilisé. IPSec via TCP se base sur la technologie NCP Path Finder. Cette technologie veille à ce que l'échange de données (IKE, ESP, AH) entre les Peers soit intégré dans une session pseudo HTTPS. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Envoyer Initial Contact Message	Indiquez si pour l'IKE (phase 1) un Initial Contact Message doit être envoyé lorsqu'aucune SA n'existe avec un Peer. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Synchroniser SAs avec l'état de l'interface ISP	Indiquez si toutes les SAs dont l'échange de données a été acheminé via une interface dont le statut est passé d' *activé* à *inactivé*, *en veille* ou *bloqué* doivent être supprimées. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Utiliser des Zero Cookies	Indiquez si des cookies ISAKMP réglés sur zéro doivent être envoyés. Ils correspondent au SPI (Security Parameter Index) dans les propositions IKE ; puisqu'ils sont redondants, ils sont normalement mis à la valeur de la négociation en cours. Votre appareil peut également utiliser des zéros pour toutes les valeurs du cookie. Sélectionnez dans ce cas le paramètre *Activé*.
Taille du Zero Cookies	Uniquement pour **Utiliser des Zero Cookies** = activé. Saisissez la longueur des SPI réglés sur zéro et utilisés dans les propositions IKE en octets. La valeur par défaut est *32*.
Authentification RADIUS dynamique	Indiquez si l'authentification RADIUS via IPSec doit être activée.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Champs du menu Options de traitement PKI

Champ	Description
Ignorer les payloads de requête de certificat	Indiquez si les demandes de certificats reçues de la partie distante pendant l'IKE (phase 1) doivent être ignorées. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Envoyer les payloads de requête de certificat	Indiquez si pendant l'IKE (phase 1) des demandes de certificats doivent être envoyées. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Envoyer la chaîne de certificats	Indiquez si pendant l'IKE (phase 1) des chaînes de certificats complètes doivent être envoyées. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut. Désactivez cette fonction si vous ne souhaitez pas envoyer les certificats de tous les niveaux (du vôtre à celui de la CA) au Peer.
Envoyer les CRL	Indiquez si pendant l'IKE (phase 1) des CRL doivent être envoyées. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Envoyer les Key Hash Payloads	Indiquez si pendant l'IKE (phase 1) des données d'identification de hachage de clé doivent être envoyées. Par défaut, le hachage de la clé publique de la partie distante est envoyé avec les autres données d'identification. Cela ne s'applique qu'au cryptage RSA. Activez cette fonction avec

Champ	Description
	Activé pour éviter un tel comportement.

13.2 L2TP

Le protocole L2TP (Layer 2 Tunneling Protocol) permet la tunnelisation de connexions PPP via une connexion UDP.

Votre appareil **Gigaset** prend en charge les deux modes suivants :

- Mode LNS L2TP (L2TP Network Server) : uniquement pour les connexions entrantes.
- Mode LAC L2TP (L2TP Access Concentrator) : uniquement pour les connexions sortantes.

Pendant la configuration du serveur et du client, il faut tenir compte des points suivants : Des deux côtés (LAC et LNS), un profil de tunnel L2TP doit être créé. Du côté du déclencheur (LAC), le profil de tunnel L2TP correspondant est utilisé pour l'établissement de la connexion. Du côté du répondant (LNS), le profil de tunnel L2TP est requis pour l'acceptation de la connexion.

13.2.1 Profils de tunnels

Dans le menu **VPN**->**L2TP**->**Profils de tunnels**, une liste de tous les profils de tunnel configurés est affichée.

13.2.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres profils de tunnel.

Le menu **VPN**->**L2TP**->**Profils de tunnels**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description pour le profil actuel. Votre appareil nomme automatiquement les profils avec *L2TP* et un numéro, cette valeur peut toutefois être modifiée.
Nom d'hôte local	Saisissez le nom d'hôte pour le LNS ou le LAC. • *LAC* : le nom d'hôte local est repris dans les messages d'établissement de tunnel sortants pour l'identification de cet appareil et est attribué au nom d'hôte distant d'un des profils

Champ	Description
	de tunnel configurés dans le LNS. Ces messages d'établissement de tunnel sont les SCCRQ (Start Control Connection Request) envoyés par le LAC et les SCCRP (Start Control Connection Reply) envoyés par le LNS. • *LNS* : correspond à la valeur de **Nom d'hôte distant** du message d'établissement de tunnel entrant du LAC.
Nom d'hôte distant	Saisissez le nom d'hôte du LNS ou du LAC. • *LAC* : définit la valeur de **Nom d'hôte local** du LNS (contenu dans les SCCRQ reçus du LNS et dans les SCCRP reçus du LAC). Un **Nom d'hôte local** configuré dans le LAC doit correspondre au **Nom d'hôte distant** configuré pour le profil prévu dans le LNS, et inversement. • *LNS* : définit le **Nom d'hôte local** du LAC. Si le champ **Nom d'hôte distant** sur le LNS reste vide, le profil correspondant est considéré comme une entrée par défaut qui est utilisée pour tous les appels entrants pour lesquels aucun profil avec un nom d'hôte distant correspondant ne peut être trouvé.
Mot de passe	Saisissez le mot de passe utilisé pour l'authentification de tunnel. L'authentification entre le LAC et le LNS s'effectue dans les deux sens : le LNS vérifie le **Nom d'hôte local** et le **Mot de passe** contenus dans le SCCRQ du LAC et les compare avec ceux mentionnés dans le profil pertinent. Le LAC fait de même avec les champs correspondants du SCCRP du LNS. Si ces champs sont laissés vides, les données d'authentification dans les messages d'établissement de tunnel ne sont ni envoyées, ni prises en compte.

Champs du menu Paramètres du mode LAC

Champ	Description
Adresse IP distante	Saisissez l'adresse IP fixe du LNS utilisée comme adresse de destination pour les connexions se basant sur ce profil. La destination doit être un appareil pouvant se comporter comme un LNS.
Port source UDP	Indiquez la méthode de détermination du numéro de port qui doit être utilisé comme port source pour toutes les connexions L2TP sortantes se basant sur ce profil.

Champ	Description
	Par défaut, l'option **Réglage fixe** est activée, ce qui signifie que des ports sont attribués de manière dynamique aux connexions utilisant ce profil. Si vous souhaitez saisir un port fixe, activez l'option *Réglage fixe*. En cas de problèmes avec le pare-feu ou le NAT, sélectionnez cette option. Les valeurs disponibles sont comprises entre *0* et *65535*.
Port de destination UDP	Saisissez le numéro de port de destination utilisé pour tous les appels se basant sur ce profil. Le LNS distant recevant l'appel doit surveiller ce port pour des connexions L2TP. Les valeurs possibles sont comprises entre *0* et *65535*. La valeur par défaut est *1701* (RFC 2661).

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Adresse IP locale	Saisissez l'adresse IP devant être utilisée en tant qu'adresse source pour toutes les connexions L2TP sortantes se basant sur ce profil. Si ce champ est laissé vide, votre appareil utilise l'adresse IP de l'interface via laquelle le tunnel L2TP joint l'adresse IP distante.
Intervalle Hello	Saisissez l'intervalle de temps (en secondes) entre l'envoi de deux messages HELLO L2TP. Ces messages servent à garder le tunnel ouvert. Les valeurs disponibles sont comprises entre *0* et *255*, la valeur par défaut est *30*. La valeur *0* signifie qu'aucun message HELLO L2TP n'est envoyé.
Temps minimal entre les tentatives	Saisissez le temps minimum (en secondes) d'attente de l'appareil avant le nouvel envoi d'un paquet de contrôle L2TP pour lequel il n'a pas reçu de réponse. Le temps d'attente est prolongé de manière dynamique jusqu'à

Champ	Description
	ce qu'il ait atteint le **Temps maximal entre les tentatives**. Les valeurs disponibles sont comprises entre `1` et `255`, la valeur par défaut est `1`.
Temps maximal entre les tentatives	Saisissez le temps maximum (en secondes) d'attente de l'appareil avant le nouvel envoi d'un paquet de contrôle L2TP pour lequel il n'a pas reçu de réponse. Les valeurs disponibles sont comprises entre `8` et `255`, la valeur par défaut est `16`.
Nombre maximal de répétitions	Indiquez le nombre maximal de tentatives de votre appareil d'envois d'un paquet de contrôle L2TP pour lequel il n'a pas reçu de réponse. Les valeurs disponibles sont comprises entre `8` et `255`, la valeur par défaut est `5`.
Numéros de séquence des paquets de données	Indiquez si votre appareil doit utiliser des numéros de séquence pour les paquets de données envoyés via un tunnel sur la base de ce profil. Sélectionnez `Activé` pour activer la fonction. La fonction est désactivée par défaut.

13.2.2 Utilisateur

Dans le menu **VPN**->**L2TP**->**Utilisateur**, une liste de tous les partenaires L2TP configurés est affichée.

13.2.2.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres partenaires L2TP.

Le menu **VPN**->**L2TP**->**Utilisateur**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez un nom pour désigner clairement le partenaire L2TP.

Champ	Description
	Dans ce champ, le premier caractère ne peut pas être un chiffre. Les caractères spéciaux et trémas ne peuvent pas non plus être utilisés. L'entrée est limitée à un maximum de 25 caractères.
Type de connexion	Indiquez si le partenaire L2TP doit jouer le rôle du serveur réseau L2TP (LNS) ou celui d'un client LAC (L2TP Access Concentrator Client). Valeurs possibles : • *LNS* (valeur par défaut) : la sélection de cette option aura pour effet la configuration du partenaire L2TP de telle sorte qu'il accepte les tunnels L2TP et rétablit le flux de données PPP encapsulé. • *LAC* : la sélection de cette option aura pour effet la configuration du partenaire L2TP de telle sorte qu'il encapsule un flux de données PPP en L2TP et établit un tunnel L2TP vers un LNS distant.
Profil de tunnel	Uniquement pour **Type de connexion** = *LAC* Sélectionnez un profil créé dans le menu **Profil de tunnel** pour la connexion vers le partenaire L2TP.
Nom de l'utilisateur	Indiquez le numéro d'identification de votre appareil.
Mot de passe	Saisissez le mot de passe.
Toujours actif	Indiquez si l'interface doit être activée en permanence. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Timeout en cas d'inactivité	Uniquement si **Toujours actif** est désactivé. Saisissez l'intervalle d'inactivité en secondes pour le shorthold statique. Vous définissez ainsi le nombre de secondes devant s'écouler entre l'envoi du dernier paquet de données et la déconnexion. Les valeurs comprises entre *0* et *3600* (secondes) sont disponibles. *0* permet de désactiver le shorthold. La valeur par dé-

Champ	Description
	faut est *300*.

Champs du menu Mode IP et routes

Champ	Description
Mode Adresse IP	Indiquez si une adresse IP statique ou dynamique doit être affectée à votre appareil. Valeurs possibles : • *Statique* (valeur par défaut) : Vous entrez une adresse IP statique. • *Mettre à disposition l'adresse IP* : uniquement pour **Type de connexion** = *LNS*. Votre appareil attribue une adresse IP dynamique au dispositif. • *Appeler l'adresse IP* : uniquement pour **Type de connexion** = *LAC*. Une adresse IP dynamique est attribuée à votre appareil.
Pool d'affectation IP (IPCP)	Uniquement pour **Mode Adresse IP** = *Mettre à disposition l'adresse IP* Sélectionnez un pool d'adresses IP configuré dans le menu **WAN**->**Internet + composer**->**Pool IP**.
Route par défaut	Uniquement pour **Mode Adresse IP** = *Appeler l'adresse IP* et *Statique* Indiquez si la route vers ce partenaire de communication doit être définie comme route par défaut. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Création entrée NAT	Uniquement pour **Mode Adresse IP** = *Appeler l'adresse IP* et *Statique* Indiquez si le NAT (Network Address Translation) doit être activé pour cette connexion. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Champ	Description
Adresse IP locale	Uniquement pour **Mode Adresse IP** = *Statique* Saisissez l'adresse WAN IP de votre appareil.
Entrées de route	Uniquement pour **Mode Adresse IP** = *Statique* Indiquez l'**Adresse IP distante** et le **Masque réseau** du LAN du partenaire L2TP et la **Métrique** correspondante. Ajoutez d'autres entrées à l'aide de l'option **Ajouter**.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Bloquer après erreur de connexion pour	Saisissez le nombre de secondes durant lesquelles aucune nouvelle tentative ne doit être effectuée à l'aide de votre appareil après un échec de connexion. La valeur par défaut est *300*.
Authentification	Sélectionnez le protocole d'authentification pour ce partenaire L2TP. Valeurs possibles : • *PAP/CHAP/MS-CHAP* (valeur par défaut) : exécuter CHAP en priorité, puis le protocole d'authentification exigé par le partenaire PPTP en cas de rejet. (MSCHAP version 1 ou 2 possible.) • *PAP* : exécuter uniquement PAP (PPP Password Authentication Protocol), le mot de passe est transmis sans cryptage. • *CHAP* : exécuter uniquement CHAP (PPP Challenge Handshake Authentication Protocol selon la RFC 1994), le mot de passe est transmis de façon cryptée. • *PAP/CHAP* : exécuter CHAP en priorité, sinon PAP. • *MS-CHAPv1* : exécuter uniquement MS-CHAP version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol). • *MS-CHAPv2*: Exécuter uniquement MS-CHAP version 2. • *aucun*: Certains fournisseurs n'utilisent pas d'authentification. Si tel est le cas, sélectionnez cette option.

Champ	Description
Cryptage	Choisissez, le cas échéant, le type de cryptage à utiliser pour l'échange de données avec le partenaire L2TP. Cela n'est possible que si la compression avec STAC ou MS-STAC n'est pas activée pour la connexion. Si l'option **Cryptage** est définie, le dispositif doit également être pris en charge pour qu'une connexion puisse être établie. Valeurs possibles : • *aucun* : aucun cryptage MPP n'est utilisé. • *Activé* (valeur par défaut) : le cryptage MPP V2 128 bits est utilisé conformément à la RFC 3078. • *Compatible Windows* : le cryptage MPP V2 128 bits est compatible avec Microsoft et Cisco.
Contrôle d'accessibilité LCP	Indiquez si l'accessibilité du dispositif doit être contrôlée par l'envoi d'Echo requests ou d'Echo replies LCP. Cette option est recommandée pour les liaisons fixes, PPTP et L2TP. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Priorétiser les paquets TCP ACK	Indiquez si le téléchargement TCP doit être optimisé en cas de chargement TCP intensif. Cette fonction est spécifiquement destinée aux bandes passantes asymétriques (ADSL). Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Champs du menu Options IP

Champ	Description
Mode OSPF	Indiquez si une propagation doit être réalisée sur les routes de l'interface et/ou si des paquets correspondant au protocole OSPF doivent être envoyés via l'interface, et de quelle manière. Valeurs possibles : • *Passif* (valeur par défaut) : OSPF n'est pas activé pour cette interface : aucune propagation n'est effectuée sur les routes associées à l'interface, et aucun paquet correspon-

Champ	Description
	dant au protocole OSPF n'est envoyé. Les réseaux accessibles via ces interfaces sont toutefois pris en compte lors du calcul des informations de routage et propagés via des interfaces actives. • *Actif* : OSPF est activé pour cette interface : une propagation est effectuée sur les routes associées à l'interface et/ou des paquets correspondant au protocole OSPF sont envoyés. • *Inactif* : OSPF est désactivé pour cette interface.
Mode Proxy ARP	Indiquez si votre appareil doit répondre aux requêtes ARP-Request de son propre LAN à la place du partenaire L2TP spécifique. Valeurs possibles : • *Inactif* (valeur par défaut) : désactive Proxy-ARP pour ce partenaire L2TP. • *Actif ou en veille* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au partenaire L2TP est *Actif* (activée) ou *En veille* (en veille). Lorsqu'il est *en veille*, votre appareil répond uniquement à la requête ARP-Request ; la connexion s'établit uniquement lorsqu'une personne souhaite utiliser la route. • *Actif uniquement* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au partenaire L2TP est *Actif* (activée), c'est-à-dire lorsqu'une connexion au partenaire L2TP est déjà établie.
Négociation DNS	Indiquez si votre appareil doit recevoir des adresses IP pour **Serveur DNS primaire** et **Serveur DNS secondaire** et **Serveur WINS Primaire** et **Secondaire** du partenaire L2TP ou envoyer celles-ci au partenaire L2TP. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

13.2.3 Options

Le menu **VPN**->**L2TP**->**Options** se compose des champs suivants :

Champs du menu Options globales

Champ	Description
Port de destination UDP	Saisissez le port devant être surveillé par le LNS pour des connexions de tunnel L2TP entrantes. Les valeurs disponibles sont tous les nombres entiers compris entre *1* et *65535*, la valeur par défaut est *1701*, conformément à la RFC 2661.
Sélection de port source UDP	Indiquez si le LNS ne doit utiliser que le port surveillé (**Port de destination UDP**) en tant que port source local pour la connexion L2TP. Sélectionnez *Réglage fixe* pour activer la fonction. La fonction est désactivée par défaut.

13.3 PPTP

Pour la protection des échanges de données via une connexion IP existante, un tunnel PPTP crypté peut être créé au moyen du protocole PPTP (Point-to-Point Tunneling Protocol).

Tout d'abord, une connexion à un ISP (Internet Service Provider) est établie sur les deux sites. Une fois ces connexions établies, un tunnel est créé via Internet vers le partenaire PPTP, dans ce cas avec PPTP.

Pour ce processus, le sous-système PPTP établit une connexion de contrôle entre les nœuds d'extrémité du tunnel. Celle-ci transmet les données de commande qui établissent, maintiennent et terminent la connexion entre les deux nœuds d'extrémité du tunnel PPTP. Dès que la connexion de contrôle est établie, le protocole PPTP transmet les données d'identification contenues dans les paquets GRE (Generic Routing Encapsulation).

13.3.1 Tunnel PPTP

Dans le menu **Tunnel PPTP**, une liste de tous les tunnels PPTP est affichée.

13.3.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres partenaires PPTP.

Le menu **VPN**->**PPTP**->**Tunnel PPTP**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres partenaire PPTP

Champ	Description
Description	Saisissez un nom pour désigner clairement le tunnel. Dans ce champ, le premier caractère ne peut pas être un chiffre. Les caractères spéciaux et trémas ne peuvent pas non plus être utilisés.
Mode PPTP	Indiquez la répartition de rôles de l'interface PPTP. Valeurs possibles : • *PNS* (valeur par défaut) : vous attribuez de la sorte à l'interface PPTP le rôle de serveur PPTP. • *Mode client Windows* : vous attribuez de la sorte à l'interface PPTP le rôle de client PPTP.
Nom de l'utilisateur	Saisissez le nom d'utilisateur.
Mot de passe	Saisissez le mot de passe.
Toujours actif	Indiquez si l'interface doit être activée en permanence. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Timeout en cas d'inactivité	Uniquement si **Toujours actif** est désactivé. Saisissez l'intervalle d'inactivité en secondes. Vous définissez ainsi le nombre de secondes devant s'écouler entre l'envoi du dernier paquet de données et la déconnexion. Valeurs possibles comprises entre *0* et *3600* (secondes). *0* permet de désactiver le Timeout. La valeur par défaut est *300*. Exemple : *10* pour les transmissions FTP, *20* pour les transmissions de LAN à LAN, *90* pour les connexions Internet.

Champ	Description
Adresse PPTP-IP distante	Uniquement pour **Mode PPTP** = *PNS* Saisissez l'adresse IP du partenaire PPTP.
Adresse PPTP-IP distante / Nom de l'hôte	Uniquement pour **Mode PPTP** = *Mode client Windows* Saisissez l'adresse IP du partenaire PPTP.

Champs du menu Mode IP et routes

Champ	Description
Mode Adresse IP	Indiquez si une adresse IP statique ou dynamique doit être affectée à votre appareil. Valeurs possibles : • *Statique* (valeur par défaut) : Vous entrez une adresse IP statique. • *Mettre à disposition l'adresse IP*: uniquement pour **Mode PPTP** = *PNS*. Votre appareil attribue une adresse IP dynamique au dispositif. • *Appeler l'adresse IP*: uniquement pour **Mode PPTP** = *Mode client Windows*. Une adresse IP dynamique est attribuée à votre appareil.
Route par défaut	Uniquement si **Mode Adresse IP** = *Statique* Indiquez si la route vers ce partenaire de communication doit être définie comme route par défaut. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Création entrée NAT	Uniquement si **Mode Adresse IP** = *Statique* Lorsqu'une connexion PPTP est configurée, indiquez si le NAT (Network Address Translation) doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Adresse IP locale	Uniquement pour **Mode Adresse IP** = *Statique*

Champ	Description
	Attribuez à l'interface PPTP l'adresse IP de votre LAN à utiliser comme adresse source interne de votre appareil.
Entrées de route	Uniquement pour **Mode Adresse IP** = *Statique* Définissez des entrées de routage pour ce partenaire de communication. • *Adresse IP distante* : adresse IP de l'hôte ou des LAN de destination. • *Masque réseau* : masque de réseau pour **Adresse IP distante**. • *Métrique* : plus faible est la valeur, plus élevée est la priorité de la route (plage de valeurs *0 - 15*). La valeur par défaut est *1*.
Pool d'affectation IP (IPCP)	Uniquement si **Mode PPTP** = *PNS*, **Mode Adresse IP** = *Mettre à disposition l'adresse IP* Sélectionnez ici un pool d'adresses IP configuré dans le menu **VPN**->**PPTP**->**Pool IP**.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Bloquer après erreur de connexion pour	Saisissez le nombre de secondes durant lesquelles aucune nouvelle tentative ne doit être effectuée à l'aide de votre appareil après un échec de connexion. La valeur par défaut est *300*.
Authentification	Sélectionnez le protocole d'authentification pour ce partenaire PPTP. Valeurs possibles : • *PAP* : exécuter uniquement PAP (PPP Password Authentication Protocol), le mot de passe est transmis sans cryptage. • *CHAP* : exécuter uniquement CHAP (PPP Challenge Handshake Authentication Protocol selon la RFC 1994), le mot de passe est transmis de façon cryptée.

Champ	Description
	• *PAP/CHAP* : exécuter CHAP en priorité, sinon PAP. • *MS-CHAPv1* : exécuter uniquement MS-CHAP version 1 (PPP-Microsoft Challenge Handshake Authentication Protocol). • *PAP/CHAP/MS-CHAP* : exécuter CHAP en priorité, puis le protocole d'authentification exigé par le partenaire PPTP en cas de rejet. (MSCHAP version 1 ou 2 possible.) • *MS-CHAPv2* (valeur par défaut) : Exécuter uniquement MS-CHAP version 2. • *aucun*: Certains fournisseurs n'utilisent pas d'authentification. Si tel est le cas, sélectionnez cette option.
Cryptage	Choisissez, le cas échéant, le type de cryptage à utiliser pour l'échange de données avec le partenaire de communication. Si l'option **Cryptage** est définie, le dispositif doit également être pris en charge pour qu'une connexion puisse être établie. Valeurs possibles : • *aucun* : aucun cryptage MPP n'est utilisé. • *Activé* (valeur par défaut) : le cryptage MPP V2 128 bits est utilisé conformément à la RFC 3078. • *Compatible Windows* : le cryptage MPP V2 128 bits est compatible avec Microsoft et Cisco.
Compression	Choisissez, le cas échéant, le type de compression à utiliser pour l'échange de données avec le partenaire de communication. Si le cryptage est défini, le dispositif doit également être pris en charge pour qu'une connexion puisse être établie. Valeurs possibles : • *aucun* (valeur par défaut) : aucun cryptage n'est utilisé. • *STAC* • *MS-STAC* • *MPPC* : Microsoft Point-to-Point Compression
Contrôle d'accessibilité LCP	Indiquez si l'accessibilité du dispositif doit être contrôlée par l'envoi d'Echo requests ou d'Echo replies LCP. Cette option est recommandée pour les liaisons fixes, PPTP et L2TP.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Champs du menu Options IP

Champ	Description
Mode OSPF	Indiquez si une propagation doit être réalisée sur les routes de l'interface et/ou si des paquets correspondant au protocole OSPF doivent être envoyés via l'interface, et de quelle manière. Valeurs possibles : • *Passif* (valeur par défaut) : OSPF n'est pas activé pour cette interface : aucune propagation n'est effectuée sur les routes associées à l'interface, et aucun paquet correspondant au protocole OSPF n'est envoyé. Les réseaux accessibles via ces interfaces sont toutefois pris en compte lors du calcul des informations de routage et propagés via des interfaces actives. • *Actif* : OSPF est activé pour cette interface : une propagation est effectuée sur les routes associées à l'interface et/ou des paquets correspondant au protocole OSPF sont envoyés. • *Inactif* : OSPF est désactivé pour cette interface.
Mode Proxy ARP	Indiquez si votre appareil doit répondre aux requêtes ARP-Request de son propre LAN à la place du partenaire PPTP spécifique. Valeurs possibles : • *Inactif* (valeur par défaut) : désactive Proxy-ARP pour ce partenaire PPTP. • *Actif ou en veille* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au partenaire PPTP est *Actif* (activée) ou *En veille* (en veille). Lorsqu'il est *en veille*, votre appareil répond uniquement à la requête ARP-Request ; la connexion s'établit uniquement lorsqu'une personne souhaite utiliser la route.

Champ	Description
	• *Actif uniquement* : votre appareil répond à une requête ARP-Request uniquement lorsque le statut de la connexion au partenaire PPTP est *Actif* (activée), c'est-à-dire lorsqu'une connexion au partenaire PPTP est déjà établie.
Négociation DNS	Indiquez si votre appareil doit recevoir des adresses IP pour **Serveur DNS primaire** et **Serveur DNS secondaire** du partenaire PPTP ou envoyer celles-ci au partenaire PPTP. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

Champs du menu PPTP-Callback

Champ	Description
Callback	Permet la mise en place d'un tunnel PPTP via Internet avec un partenaire PPTP, même si ce dernier est momentanément hors ligne. En règle générale, le partenaire PPTP est invité au moyen d'un appel RNIS à se connecter et à établir une connexion PPTP. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Notez que vous devez activer l'option correspondante sur les passerelles des deux partenaires. Cette fonction requiert en règle générale une connexion RNIS. Sans RNIS, le Callback ne peut être activé que dans des applications spéciales.
Numéro RNIS entrant	Uniquement si **Callback** est activé. Indiquez le numéro RNIS à partir duquel l'appareil distant appelle l'appareil local (Calling Party Number).
Numéro RNIS sortant	Uniquement si **Callback** est activé. Indiquez le numéro RNIS sous lequel l'appareil local appelle l'appareil distant (Called Party Number).

Champs du menu Sélection du port de composition (uniquement lorsque le Callback est activé)

Champ	Description
Ports sélectionnés	Saisissez les ports RNIS par lesquels le Callback doit être ef-

Champ	Description
	fectué. Valeurs possibles : • *Tous les ports* : le Callback est effectué par l'un des ports RNIS disponibles. • *Saisir le port* : vous pouvez sélectionner les ports RNIS souhaités dans **Ports spécifiques**.
Ports spécifiques	Vous ne pouvez sélectionner d'autres ports avec le bouton **Ajouter** que pour **Ports sélectionnés** = *Saisir le port*.

13.3.2 Options

Dans ce menu, vous pouvez effectuer des paramétrages généraux du profil PPTP global.

Le menu **VPN**->**PPTP**->**Options** se compose des champs suivants :

Champs du menu Options globales

Champ	Description
Adaptation GRE-Window	Indiquez si vous souhaitez activer l'adaptation GRE-Window. Cette modification n'est nécessaire que si vous avez installé le Service Pack 1 dans Microsoft Windows XP. Microsoft ayant modifié avec le SP1 l'algorithme de confirmation dans le protocole GRE, la mise à jour automatique des fenêtres pour GRE doit être désactivée sur les appareils **Gigaset**. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Taille GRE-Window	Indiquez le nombre maximal de paquets GRE pouvant être envoyés sans confirmation. Windows utilise depuis la version XP une fenêtre de réception initiale plus élevée dans GRE, raison pour laquelle la taille de fenêtre d'envoi maximale doit être adaptée au moyen de la valeur **Taille GRE-Window**. Les valeurs possibles sont comprises entre *0* et *256*. La valeur par défaut est *0*.
Connexions de	Indiquez le nombre maximal de connexions de contrôle.

Champ	Description
contrôle entrantes max via adresse IP distante	

13.3.3 Pool IP

Dans le menu **Pool IP**, une liste de tous les pools IP pour les connexions PPTP est affichée.

Votre appareil peut faire fonction de serveur d'adresses IP dynamique pour les connexions PPTP. Pour ce faire, mettez un ou plusieurs pools d'adresses IP à disposition. Ces adresses IP peuvent être attribuées à des partenaires de communication connectés pour la durée de la communication.

Les routes d'hôtes saisies ont toujours la priorité sur les adresses IP des pools d'adresses. Ainsi, lorsqu'un appel entrant a été authentifié, votre appareil vérifie d'abord si une route d'hôte a été saisie dans le tableau de routage pour l'appelant. Si tel n'est pas le cas, votre appareil peut attribuer une adresse IP issue d'un pool d'adresses (si disponible). Dans le cas de pools d'adresses contenant plusieurs adresses IP, vous ne pouvez pas déterminer les adresses à attribuer aux partenaires de communication. Les adresses sont d'abord simplement attribuées dans l'ordre indiqué. Lors d'une nouvelle tentative de connexion dans un intervalle d'une heure, le système tente de nouveau d'affecter l'adresse IP attribuée en dernier lieu à ce partenaire.

Sélectionnez le bouton **Ajouter** pour configurer d'autres pools IP.

13.3.3.1 Editer ou Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres pools d'adresses IP. Sélectionnez le symbole pour traiter les entrées existantes.

Champs du menu Paramètres de base

Champ	Description
Nom de pool IP	Saisissez une description pour désigner clairement le pool d'adresses IP.
Plage d'adresses IP	Saisissez la première (premier champ) et la dernière (deuxième champ) adresse IP du pool d'adresses IP.
Serveur DNS	**Primaire** : saisissez l'adresse IP du serveur DNS qui doit être utilisé de préférence par les clients qui reçoivent une adresse

Champ	Description
	issue de ce pool d'adresses. **Secondaire** : saisissez l'adresse IP d'un autre serveur DNS.

13.4 GRE

Le GRE (Generic Routing Encapsulation) est un protocole de réseau servant à encapsuler d'autres protocoles et à les transporter ainsi sous forme de tunnels IP vers des destinataires spécifiques.

La spécification du protocole GRE est disponible en deux versions :

- GRE V.1 pour une utilisation dans des connexions PPTP (RFC 2637, configuration dans le menu **PPTP**)
- GRE V.0 (RFC 2784) pour un encapsulage général au moyen de GRE

Dans ce menu, vous pouvez configurer une interface virtuelle pour l'utilisation de GRE V.0. L'échange de données acheminé via cette interface est ensuite encapsulé au moyen de GRE et envoyé au destinataire spécifique.

13.4.1 Tunnel GRE

Dans le menu **VPN**->**GRE**->**Tunnel GRE**, une liste de tous les tunnels GRE configurés est affichée.

13.4.1.1 Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres tunnels GRE.

Le menu **VPN**->**GRE**->**Tunnel GRE**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description pour le tunnel GRE.
Adresse GRE-IP locale	Saisissez l'adresse IP source des paquets GRE vers le partenaire GRE. Si aucune adresse IP n'est saisie (correspond à l'adresse IP 0.0.0.0), l'adresse IP source des paquets GRE est sélectionnée automatiquement parmi les adresses des interfaces par lesquelles ce partenaire GRE est joint.

Champ	Description
Adresse GRE-IP distante	Saisissez l'adresse IP de destination des paquets GRE vers le partenaire GRE.
Route par défaut	Si vous activez l'option **Route par défaut**, toutes les données sont automatiquement transmises vers une connexion. La fonction est désactivée par défaut.
Adresse IP locale	Saisissez ici l'adresse IP (du côté LAN) devant être utilisée par votre appareil en tant qu'adresse source pour des paquets propres par le tunnel GRE.
Entrées de route	Définissez d'autres entrées de routage pour ce partenaire de communication. Ajoutez de nouvelles entrées à l'aide de l'option **Ajouter**. • *Adresse IP distante* : adresse IP de l'hôte ou du réseau de destination. • *Masque réseau* : masque de réseau pour **Adresse IP distante**. En l'absence de saisie, votre appareil utilise un masque de réseau par défaut. • *Métrique* : plus la valeur est faible, plus la priorité de la route est élevée (plage de valeurs *0*... *15*). La valeur par défaut est *1*.
MTU	Saisissez la taille maximale de paquet (Maximum Transfer Unit, MTU) en octets pouvant être utilisée pour la connexion GRE entre les partenaires. Les valeurs possibles sont comprises entre *1* et *8192*. La valeur par défaut est *1500*.
Utiliser la clé	Activez la saisie d'un numéro d'identification pour la connexion GRE afin de permettre la distinction de plusieurs connexions GRE en parallèle entre deux partenaires GRE (voir RFC 1701). Sélectionnez *Activé* pour activer le numéro d'identification. La fonction est désactivée par défaut.
Valeur de la clé	Uniquement si **Utiliser la clé** est activé.

Champ	Description
	Indiquez le numéro d'identification de connexion GRE. Les valeurs possibles sont comprises entre *0* et *2147483647*. La valeur par défaut est *0*.

Chapitre 14 Pare-feu

Avec un pare-feu « Stateful Inspection Firewall » (SIF) les passerelles **Gigaset** disposent d'une fonction de sécurité performante.

Outre le filtrage de paquets dit statique, un SIF présente un avantage décisif grâce au filtrage de paquets dynamique. La décision quant à la transmission ou non d'un paquet ne peut pas seulement être prise en raison des adresses source et cible ou des ports, mais aussi à l'aide du filtrage de paquets dynamique selon l'état (statut) de la connexion avec un partenaire.

Cela permet de transmettre aussi des paquets appartenant à une connexion déjà active. Dans ce cas, le SIF accepte même les paquets appartenant à une « connexion esclave ». La négociation d'une connexion FTP par ex. a lieu via le port 21, alors que l'échange réel des données peut être effectué via un autre port.

SIF et les autres fonctions de sécurité

En raison de sa configuration simple, le pare-feu « Stateful Inspection Firewall » s'insère aisément dans l'architecture de sécurité des appareils **Gigaset**. Par rapport aux systèmes tels que la « Network Adress Translation » (NAT et les listes d'accès IP (IPAL), la configuration du SIF est relativement simple.

Comme SIF, NAT et IPAL sont actifs simultanément dans le système, il convient de veiller aux interactions éventuelles : Si un paquet quelconque est rejeté par l'une des instances de sécurité, le rejet est direct, c'est-à-dire que l'acceptation éventuelle du paquet par une autre instance est sans importance. Il convient donc d'analyser en détail ses besoins en fonctions de sécurité.

La différence essentielle entre SIF et NAT/IPAL consiste en le fait que les règles du SIF sont appliquées généralement de manière globale, c'est-à-dire qu'elles ne sont pas limitées à une interface.

Par principe, les mêmes critères de filtration sont appliquées au trafic de données que pour NAT et IPAL :

- Adresses source et cible du paquet (avec un masque de réseau correspondant).
- Service (préconfiguré, par ex. Echo, FTP, HTTP).
- Protocole
- Numéro(s) de port(s)

Pour illustrer les différences du filtrage des paquets, vous trouverez ci-dessous une liste

des différentes instances de sécurité et de leur mode de fonctionnement.

NAT

Une des fonctions de base de NAT est la conversion des adresses IP locales de votre LAN vers les adresses IP globales qui vous sont affectées par votre IPS, et inversement. Dans ce contexte, toutes les connexions initiées de l'extérieur sont bloquées, c'est-à-dire que chaque paquet que votre appareil ne peut pas affecter à une connexion déjà existante est refusé. Ainsi, la connexion ne peut être établie que de l'intérieur vers l'extérieur. Sans autorisations explicites, NAT rejette tout accès du WAN sur le LAN.

Listes d'accès IP

Ici, les paquets sont admis ou refusés exclusivement en raison des critères décrits ci-dessus, c'est-à-dire que l'état de la connexion n'est pas pris en compte (sauf pour **Services** = *TCP*).

SIF

Le SIF refuse tous les paquets qui ne sont pas autorisés explicitement ou implicitement. Il procède à des « refus », pour lesquels aucun message d'erreur n'est renvoyé à l'expéditeur du paquet refusé, mais aussi à des « rejets » pour lesquels l'expéditeur est informé du rejet du paquet.

Les paquets entrants sont traités comme suit :

- D'abord le SIF vérifie si un paquet entrant peut être affecté à une connexion existante. Si cela est le cas, il est transmis. Si le paquet ne peut être attribué à aucune connexion existante, le SIF vérifie si une telle connexion peut être attendue (par ex. comme connexion esclave d'une connexion existante). Si cela est le cas, le paquet est également accepté.
- Si le paquet ne peut être attribué à aucune connexion existante ou pouvant être attendue, les règles de filtrage SIF sont appliquées : Si le paquet fait l'objet d'une règle de refus, il est refusé sans qu'un message d'erreur ne soit envoyé à l'expéditeur du paquet ; si une règle de rejet s'applique, le paquet est rejeté et un message ICMPHost Unreachable est émis à l'attention de l'expéditeur. Le paquet n'est transmis que si une règle d'acceptation s'applique à lui.
- Tous les paquets auxquels aucune règle ne s'applique sont rejetés après contrôle de toutes les règles existantes, sans qu'un message d'erreur ne soit envoyé à l'expéditeur (= comportement standard).

14.1 Directives

14.1.1 Règles de filtre

Le comportement standard avec l'**Action** = *Accès* se compose de deux règles de filtrage implicites : si un paquet entrant peut être affecté à une connexion existante et si une connexion correspondante peut être attendue (par ex. comme connexion esclave d'une connexion existante), le paquet est accepté.

La séquence des règles de filtrage dans la liste est importante : Les règles de filtrage sont appliquées dans l'ordre à chaque paquet jusqu'à ce que l'une des règles de filtrage corresponde. En cas de chevauchements, c'est-à-dire si plus d'une règle de filtrage s'applique à un paquet, seul la première règle de filtrage est exécutée. Si donc la première règle de filtrage rejette le paquet, tandis qu'une règle ultérieure l'accepte, il est néanmoins refusé. De même une règle de refus reste sans effet si un paquet est accepté auparavant par une autre règle de filtrage.

Le menu **Pare-feu**->**Directives**->**Règles de filtre** contient la liste de toutes les règles de filtrage configurées.

Le bouton permet d'insérer une directive supplémentaire au-dessus de la ligne de la liste. Un menu de configuration s'affiche pour créer une nouvelle directive.

Le bouton permet de déplacer l'entrée de la liste. Un dialogue s'affiche, dans lequel vous pouvez choisir la position sur laquelle la directive est déplacée.

14.1.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres paramètres.

Le menu **Pare-feu**->**Directives**->**Règles de filtre**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Source	Sélectionnez l'un des alias préconfigurés pour la source du paquet. La liste contient toutes les interfaces WAN/LAN, tous les groupes d'interfaces (voir **Pare-feu**->**Interfaces**->**Groupes**), les adresses (voir **Pare-feu**->**Adresses**->**Liste d'adresses**) et

Champ	Description
	groupes d'adresses (voir **Pare-feu**->**Adresses**->**Groupes**) au choix. La valeur *Quelconque* signifie que si l'interface source, ni l'adresse source ne sont contrôlées.
Destination	Sélectionnez l'un des alias préconfigurés pour la ciblé du paquet. la liste contient toutes les interfaces WAN/LAN, tous els groupes d'interfaces (voir **Pare-feu**->**Interfaces**->**Groupes**), les adresses (voir **Pare-feu**->**Adresses**->**Liste d'adresses**) et les groupes d'adresses (voir **Pare-feu**->**Adresses**->**Groupes**) au choix. La valeur *Quelconque* signifie que si l'interface cible, ni l'adresse cible ne sont contrôlées.
Service	Sélectionnez l'un des services préconfigurés auxquels le paquet à filtrer doit être affecté. D'origine, une liste complète de services est préconfigurée, dont : • *ftp* • *telnet* • *smtp* • *dns* • *http* • *nntp* • *Internet* • *Netmeeting* D'autres services sont créés dans **Pare-feu**->**Services**->**Liste de services**. De plus, les groupes de services configurés dans **Pare-feu**->**Services**->**Groupes** sont également disponibles au choix.
Action	Choisissez une action à appliquer à un paquet filtré. Valeurs possibles :

Champ	Description
	• *Accès* (valeur par défaut) : Les paquets sont transmis en fonction des indications. • *Refuser*: les paquets sont refusés. • *Rejeter*: les paquets sont refusés. Un message d'erreur est envoyé à l'expéditeur du paquet.
Appliquer QoS	Uniquement pour **Action** = *Accès* Choisissez si vous souhaitez activer QoS pour cette directive avec la priorité sélectionnée dans **Priorité**. Sélectionnez *Activé* pour activer la fonction. L'option est désactivée par défaut. Si QoS n'est pas actif pour cette directive, la priorisation des données n'est pas non plus possible du côté expéditeur. Une directive pour laquelle QoS a été activé est paramétrée aussi pour le pare-feu. Notez que dans le cas, le trafaic de données qui n'a pas été explicitement accepté sera bloqué par le pare-feu !
Priorité	Uniquement pour **Action** = *Accès* et **Appliquer QoS** = *Activé* Choisissez la priorité avec laquelle les données spécifiées par la directive devront être traitées du côté de l'expéditeur. Valeurs possibles : • *aucun* (valeur par défaut) : Aucune priorité. • *Low Latency*: Low Latency Transmission (LLT), c'est-à-dire le traitement des données avec la latence maximale, par ex. pour les données VoIP. • *Haut* • *Moyen* • *bas*

14.1.2 QoS

De plus en plus d'applications ont besoin de bandes de plus en plus larges. Celles-ci ne sont pas toujours disponibles. « Quality of Service » (QoS) permet de répartir les largeurs de bandes disponibles de manière efficace et intelligente. Certaines applications peuvent être traitées de manière préférentielle et de la largeur de bande peut être réservée pour elles.

Le menu **Pare-feu**->**Directives**->**QoS** contient la liste de toutes les règles QoS.

14.1.2.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres règles QoS.

Le menu **Pare-feu**->**Directives**->**QoS**->**Nouveau** se compose des champs suivants :

Champs du menu Configurer l'interface QoS

Champ	Description
Interface	Choisissez l'interface sur laquelle la gestion de largeur de bande doit être réalisée.
Traffic Shaping	Choisissez si vous souhaitez activer la gestion de largeur de bande pour l'interface sélectionnée. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Saisir la bande passante	Uniquement pour **Traffic Shaping** = *Activé* Saisissez en kbits/s la largeur de bande maximale disponible pour l'interface sélectionnée.
Règles de filtre	Ce champ contient une liste de toutes les directives de pare-feu pour lequelles QoS a été activé (**Appliquer QoS** = *Activé*). Pour chaque entrée de liste, les options suivantes sont disponibles : • **Utilisateur**: Indiquez si cette entrée doit être affectée à l'interface QoS. Cette option est désactivée par défaut. • **Bande passante**: Saisissez en kbits/s la largeur de bande maximale disponible pour le service indiqué sous **Service**. La valeur par défaut est *0*.

Champ	Description
	• **Fixe**: Choisissez si un dépassement durable de la largeur de bande définie dans **Bande passante** est admissible. L'activation de ce champ exclut un tel dépassement. Si l'option est désactivée, le dépassement est autorisé et la vitesse de transfert de données excédentaire est traitée selon la priorité définie dans la directive de pare-feu correspondante. Cette option est désactivée par défaut.

14.1.3 Options

Ce menu permet d'activer ou de désactiver le pare-feu et l'enregistrement d'un compte-rendu de ses activités. De plus, vous pouvez définir après combien de secondes d'inactivité une session sera terminée.

Le menu **Pare-feu**->**Directives**->**Options** se compose des champs suivants :

Champs du menu Options générales pare-feu

Champ	Description
État du pare-feu	Activez ou désactivez la fonction de pare-feu. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Actions journalisées	Sélectionnez le niveau syslog pare-feu. La sortie du message s'effectue simultanément à celle des messages des autres sous-systèmes. Valeurs possibles : • *Tous* (valeur par défaut) : Toutes les activités de pare-feu s'affichent. • *Refuser*: Seuls les événements de rejet et de refus s'affichent, comparer avec « Action ». • *Accepter*: Seuls les événements d'acceptation s'affichent. • *aucun*: Aucun message de protocole système n'est généré.
Filtrage complet	Ici, vous pouvez définir si seuls les paquets sont filtrés qui sont envoyés à une autre interface que celle ayant établi la connexion.

Champ	Description
	L'option *Activer* entraîne le filtrage de tous les paquets (standard).

Champs du menu Horloge de session

Champ	Description
Inactivité UDP	Indiquez après combien de temps d'inactivité une session USP sera considérée comme écoulée (en secondes). Les valeurs comprises entre *30* et *86400* sont disponibles. La valeur par défaut est *180*.
Inactivité TCP	Indiquez après combien de temps d'inactivité une session TCP sera considérée comme écoulée (en secondes). Les valeurs comprises entre *30* et *86400* sont disponibles. La valeur par défaut est *3600*.
Inactivité PPTP	Indiquez après combien de temps d'inactivité une session PPTP sera considérée comme écoulée (en secondes). Les valeurs comprises entre *30* et *86400* sont disponibles. La valeur par défaut est *86400*.
Autre inactivité	Indiquez après combien de temps d'inactivité une session d'un autre type sera considérée comme écoulée (en secondes). Les valeurs comprises entre *30* et *86400* sont disponibles. La valeur par défaut est *30*.

14.2 Interfaces

14.2.1 Groupes

Le menu **Pare-feu**->**Interfaces**->**Groupes** contient la liste de tous les groupes d'interfaces configurés.

Vous pouvez rassembler les interfaces de votre appareil en groupes. Ceci simplifie la

configuration des règles de pare-feu.

14.2.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres groupes d'interfaces.

Le menu **Pare-feu**->**Interfaces**->**Groupes**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description quelconque du groupe d'interfaces.
Membres	Choisissez les membres du groupe parmi les interfaces disponibles. Pour ce faire, activez le champ dans la colonne **Sélection**.

14.3 Adresses

14.3.1 Liste d'adresses

Le menu **Pare-feu**->**Adresses**->**Liste d'adresses** contient la liste de toutes les adresses configurées.

14.3.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres adresses.

Le menu **Pare-feu**->**Adresses**->**Liste d'adresses**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description quelconque de l'adresse.
Type d'adresse	Choisissez le type d'adresse que vous souhaitez indiquer. Valeurs possibles : • *Adresse/Sous-réseau* (valeur par défaut) : Vous saisissez une adresse IP avec masque de sous-réseau.

Champ	Description
	• *Plage d'adresses*: Vous saisissez une plage d'adresses IP avec adresse initiale et adresse finale.
Adresse/Sous-réseau	Uniquement pour **Type d'adresse** = *Adresse/Sous-réseau* Saisissez l'adresse IP de l'hôte ou une adresse réseau, ainsi que le masque de réseau correspondant. La valeur par défaut est respectivement *0.0.0.0*.
Plage d'adresses	Uniquement pour **Type d'adresse** = *Plage d'adresses* Saisissez l'adresse IP de début et de fin de la plage.

14.3.2 Groupes

Le menu **Pare-feu**->**Adresses**->**Groupes** contient la liste de tous les groupes d'adresses configurés.

Vous pouvez rassembler les adresses en groupes. Ceci simplifie la configuration des règles de pare-feu.

14.3.2.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres groupes d'adresses.

Le menu **Pare-feu**->**Adresses**->**Groupes**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description quelconque du groupe d'adresses.
Sélection	Choisissez les membres du groupe parmi les **Adresses** disponibles. Pour ce faire, activez le champ dans la colonne **Sélection**.

14.4 Services

14.4.1 Liste de services

Le menu **Pare-feu**->**Services**->**Liste de services** contient la liste de tous les services disponibles.

14.4.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres services.

Le menu **Pare-feu**->**Services**->**Liste de services**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez un alias pour le service que vous souhaitez configurer.
Journal	Choisissez le protocole sur lequel le service doit reposer. Les protocoles principaux sont disponibles au choix.
Plage de port de destination	Uniquement pour **Journal** = *TCP*, *UDP/TCP* ou *UDP* Saisissez dans le premier champ le port cible via lequel le service sera exécuté. Si vous souhaitez indiquer une plage de numéros de ports, indiquez le cas échéant dans le second champ le dernier port d'une plage de ports. Par défaut, le champ ne contient aucune entrée. Si une valeur s'affiche, cela signifie que le numéro de port renseigné précédemment est en cours de vérification. Si une plage de ports est vérifiée, vous devez saisir une limite. Les valeurs possibles sont comprises entre *1* et *65535*.
Plage de port source	Uniquement pour **Journal** = *TCP*, *UDP/TCP* ou *UDP* Saisissez dans le premier port le port source à contrôler éventuellement. Si vous souhaitez indiquer une plage de numéros de ports, indiquez le cas échéant dans le second champ le dernier port d'une plage de ports. Par défaut, le champ ne contient aucune entrée. Si une valeur s'affiche, cela signifie que le numéro de

Champ	Description
	port renseigné précédemment est en cours de vérification. Si une plage de ports est vérifiée, vous devez saisir une limite. Les valeurs possibles sont comprises entre *1* et *65535*.
Type	Uniquement pour **Journal** = *ICMP* Le champ **Type** indique la classe des messages ICMP, tandis que le champ **Code** fournit plus de précisions sur le type de messages. Valeurs possibles : • *Quelconque* (valeur par défaut) • *Echo Reply* • *Destination Unreachable* • *Source Quench* • *Rediriger* • *Echo* • *Time Exceeded* • *Problème de paramètres* • *Timestamp* • *Timestamp Reply* • *Information Request* • *Information Reply* • *Address Mask Request* • *Address Mask Reply*
Code	Vous ne disposez d'un choix pour le code ICMP que pour **Type** = *Destination Unreachable*. Valeurs possibles : • *Quelconque* (valeur par défaut) • *Net Unreachable* • *Host Unreachable* • *Protocol Unreachable* • *Port Unreachable*

Champ	Description
	• *Fragmentation Needed* • *Communication with Destination Network is Administratively Prohibited* • *Communication with Destination Host is Administratively Prohibited*

14.4.2 Groupes

Le menu **Pare-feu**->**Services**->**Groupes** contient la liste de tous les groupes de services configurés.

Vous pouvez rassembler les services en groupes. Ceci simplifie la configuration des règles de pare-feu.

14.4.2.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres groupes de services.

Le menu **Pare-feu**->**Services**->**Groupes**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une description quelconque du groupe de services.
Membres	Choisissez les membres du groupe parmi les alias de services disponibles. Pour ce faire, activez le champ dans la colonne **Sélection**.

Chapitre 15 Services locaux

Ce menu met à disposition des services pour les groupes de thèmes suivants :

- Conversion des noms (DNS)
- Configuration par navigateur Internet (HTTPS)
- Recherche dynamique d'adresses IP à l'aide d'un fournisseur d'accès DynDNS
- Configuration de la passerelle comme serveur DHCP (attribution d'adresses IP)
- Automatisation des tâches selon un planning temporel (planification)
- Contrôles de joignabilité des hôtes ou interfaces, test Ping
- Vidéo en temps réel / conférences audio (services de messagerie, Plug & Play universel)
- Mise à disposition d'accès Internet publics (Hotspots)
- Wake on LAN pour l'activation d'appareils réseau qui sont actuellement désactivés.

15.1 DNS

Chaque appareil d'un réseau TCP/IP est normalement adresse à l'aide de son adresse IP. Comme dans les réseau, les noms d'hôtes sont souvent utilisés pour s'adresser à différents appareils, l'adresse IP correspondante doit être communiquée. Cette tâche est par ex. remplie par un serveur DNS. Il convertit les noms d'hôtes en adresses IP. Alternativement, la conversion du nom peut aussi être réalisée à l'aide du fichier HOSTS qui figure sur tous les ordinateurs.

Votre appareil offre les possibilités suivantes pour la conversion des noms :

- Un proxy DNS pour transmettre les demandes de DNS adresses à votre appareil vers un serveur DNS approprié. Cela inclut aussi la transmission spécifique de domaines définis (transmission de domaines).
- Un cache DNS pour enregistrer les résultats positifs et négatifs des demandes DNS.
- Des entrées statiques (hôtes statiques) pour définir ou empêcher manuellement l'attribution d'adresses IP.
- La surveillance DNS (statistiques) pour obtenir une vue d'ensemble des demandes DNS sur votre appareil.

Serveur de noms

Sous **Services locaux**->**DNS**->**Paramètres globaux**->**Paramètres de base** figurent les

adresses IP de serveurs de noms qui sont interrogés lorsque votre appareil ne peut pas répondre lui-même ou par des entrées de transmission à des demandes. Il est possible de saisir des serveurs de noms globaux, mais aussi des serveurs de noms liés à une interface.

Votre appareil peut aussi obtenir ou transmettre dynamiquement les adresses des serveurs de noms globaux, via PPP ou DHCP.

Stratégie de conversion des noms sur votre appareil

Votre appareil traite les demandes DNS de la manière suivante :

(1) Si possible, votre appareil répond aux demandes depuis le cache statique ou dynamique en fournissant directement l'adresse IP ou une réponse négative.

(2) D'autre part, si une entrée de transmission appropriée est disponible, le serveur DNS correspondant est interrogé, en fonction de la configuration des connexions Internet ou de numérotation, le cas échéant après établissement d'une connexion WAN payante. Si le serveur DNS parvient à résoudre le nom, les informations sont transmises et une entrée dynamique est créée dans le cache.

(3) Dans le cas contraire, si le nom du serveur est entré, le serveur DNS primaire, puis le serveur DNS secondaires sont interrogés en tenant compte de la priorité configurée et si l'état de l'interface correspondant est « up ». Si l'un des serveurs DNS parvient à résoudre le nom, les informations sont transmises et une entrée dynamique est créée dans le cache.

(4) D'autre part, si une une connexion Internet ou à numérotation est sélectionnée comme interface standard, les serveurs DNS correspondants sont interrogés, en fonction de la configuration des connexions Internet ou de numérotation, le cas échéant après établissement d'une connexion WAN payante. Si l'un des serveurs DNS parvient à résoudre le nom, les informations sont transmises et une entrée dynamique est créée dans le cache.

(5) D'autre part, si dans le menu **WAN**->**Internet + composer** une entrée a été créée et que l'écrasement d'adresses des serveurs de noms globaux est autorisé (**Mode interfaces** = *Dynamique*), une connexion est établie avec la première connexion Internet ou à numérotation, le cas échéant moyennant paiement, qui est configurée de sortie que les adresses de serveurs DNS puissent être demandées par des serveurs DNS (**Négociation DNS** = *Activé*), dans la mesure où cela n'a pas été tenté auparavant. Après une négociation de serveur de noms réussie, ce serveur de noms est alors disponible pour d'autres demandes à venir.

(6) Dans le cas contraire, la demande initiale déclenche une erreur de serveur.

Si un des serveurs DNS répond par `Domaine inexistant`, la demande initiale reçoit immédiatement une réponse correspondante et une entrée négative appropriée est enregistrée dans le cache DNS de votre appareil.

15.1.1 Paramètres globaux

Le menu **Services locaux**->**DNS**->**Paramètres globaux** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Nom de domaine	Indiquez le nom de domaine par défaut de votre appareil.
Serveur WINS **Primaire** **Secondaire**	Saisissez l'adresse IP du premier, et le cas échéant d'un second serveur global « Windows Internet Name Server (WINS) ou serveur « NetBIOS Name Server (NBNS).

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Cache positif	Choisissez si le cache dynamique positif doit être activé, c'est-à-dire si les noms et adresses IP résolus avec succès doivent être enregistrés dans le cache. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Cache négatif	Choisissez si le cache dynamique négatif doit être activé, c'est-à-dire si les demandes de noms pour lesquels un serveur DNS a envoyé une réponse négative doivent être enregistrées dans le cache comme entrées négatives. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Taille du cache	Saisissez le nombre total maximal des entrées statiques et dynamiques. Lorsque cette valeur est atteinte, l'entrée dynamique qui n'a pas été interrogée depuis le plus longtemps sera écrasée par la nouvelle entrée. Si la **Taille du cache** est diminuée par

Champ	Description
	l'utilisateur, certaines entrées dynamique seront également supprimées le cas échéant. Les entrées statiques ne sont pas supprimées. **Taille du cache** ne peut pas être réduit à une taille inférieure au nombre actuellement présent d'entrées statiques. Valeurs possibles : *0*.. *1000*. La valeur par défaut est *100*.
TTL maximal pour entrées cache positives	Saisissez la valeur à laquelle le TTL pour une entrée DNS dynamique positive doit être définie dans le cache, si son TTL est de *0* ou si son TTL dépasse la valeur pour **TTL maximal pour entrées cache positives**. La valeur par défaut est *86400*.
TTL maximal pour entrées cache négatives	Saisissez la valeur à laquelle le TTL doit être réglé en cas d'entrée dynamique négative dans le cache. La valeur par défaut est *86400*.
Interface alternative pour recevoir le serveur DNS	Choisissez l'interface vers laquelle une connexion de négociation de serveur de noms est établie lorsque les autres tentatives de résolution de nom ont échoué. La valeur par défaut est *Automatique*, c'est-à-dire qu'une connexion est établie une fois vers le premier partenaire de connexion approprié configuré dans le réseau.

Champs du menu Adresse IP à utiliser pour l'affectation de serveur DNS-/WINS

Champ	Description
En tant que serveur DHCP	Sélectionnez les adresses de serveurs de noms transmises au client DHCP si votre appareil est utilisé comme serveur DHCP. Valeurs possibles : • *aucun*: Aucune adresse de serveur de noms n'est transmise. • *Adresse IP propre* (valeur par défaut) : L'adresse de votre appareil est transmise comme adresse de serveur de noms. • *Paramètres DNS*: Les adresses des serveurs de noms glo-

Champ	Description
	baux enregistrées sur votre appareil sont transmises.
En tant que serveur IPCP	Choisissez les adresses de serveurs de noms qui seront transmises par votre appareil en cas de négociation de serveur de noms dynamique si votre appareil est utilisé comme serveur IPCP pour les connexions PPP. Valeurs possibles : • *aucun*: Aucune adresse de serveur de noms n'est transmise. • *Adresse IP propre*: L'adresse de votre appareil est transmise comme adresse de serveur de noms. • *Paramètres DNS* (valeur par défaut) : Les adresses des serveurs de noms globaux enregistrées sur votre appareil sont transmises.

15.1.2 Serveur DNS

Le menu **Services locaux**->**DNS**->**Serveur DNS** affiche la liste de tous les serveurs DNS configurés.

15.1.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres serveurs DNS.

Vous pouvez configurer ici des serveurs DNS globaux, ainsi que des serveurs DNS devant être affectés à une interface spécifique.

La configuration d'un serveur DNS pour une interface spécifique peut être utile par exemple si des comptes de différents fournisseurs d'accès sont installés sur différentes interfaces et que la répartition de la charge est utilisée.

Le menu **Services locaux**->**DNS**->**Serveur DNS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
État admin	Indiquez si le serveur DNS doit être activé.

Champ	Description
	Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Description	Saisissez une description pour le serveur DNS.
Priorité	Affectez une priorité au serveur DNS. Vous pouvez affecter à une interface (c'est-à-dire par ex. à un port Ethernet ou un partenaire PPPoE WAN) plusieurs paires de serveurs DNS (**Serveur DNS primaire** et **Serveur DNS secondaire**). La paire avec la priorité la plus élevée est utilisé lorsque l'interface est à l'état « up ». Valeurs possibles comprises entre *0* (priorité la plus haute) et *9* (priorité la plus basse). La valeur par défaut est *5*.
Mode interfaces	Choisissez si les adresses IP de serveurs de noms pour la résolution des noms des adresses Internet sont obtenues automatiquement ou si, en fonction de la priorité, jusqu'à deux adresses de serveur DNS fixes doivent être saisies. Valeurs possibles : • *Statique* • *Dynamique* (valeur par défaut)
Interface	Choisissez l'interface à laquelle la paire de serveurs DNS doit être affectée. Si **Mode interfaces** = *Dynamique* Le réglage *Aucune* entraîne la création d'un serveur DNS global. Si **Mode interfaces** = *Statique* Le réglage *Quelconque* conduite à la configuration d'un serveur DNS pour toutes les interfaces.
Serveur DNS primaire	Uniquement si **Mode interfaces** = *Manuel* Saisissez l'adresse IP du premier serveur de noms pour la ré-

Champ	Description
	solution des noms des adresses Internet.
Serveur DNS secondaire	Uniquement si **Mode interfaces** = *Manuel* Si vous le souhaitez, saisissez l'adresse IP d'un autre serveur de noms.

15.1.3 Hôtes statiques

Le menu **Services locaux**->**DNS**->**Hôtes statiques** affiche la liste de tous les hôtes statiques configurés.

15.1.3.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres hôtes statiques.

Le menu **Services locaux**->**DNS**->**Hôtes statiques**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Nom d'hôte DNS	Saisissez le nom de l'hôte auquel l'**Adresse IP** configurée dans ce menu doit être affectée lorsqu'une demande DNS obtient une réponse positive. Si une demande DNS obtient une réponse négative, aucune adresse n'est communiquée. L'entrée peut aussi débuter par un caractère de substitution, par ex. *.bintec-elmeg.com. Lors de la saisie d'un nom sans point, le système le complète après confirmation par **OK** « <**Name**.> ». Les entrées avec des espaces ne sont pas autorisées.
Réponse	Sélectionnez le type de réponses aux demandes DNS pour cette entrée. Valeurs possibles : • *Négatif*: Une demande DNS de **Nom d'hôte DNS** obtient une réponse négative. • *Positif* (valeur par défaut) : Une demande DNS de **Nom**

Champ	Description
	d'hôte DNS obtient comme réponse l'**Adresse IP** correspondante. • *aucun*: Une demande DNS est ignorée et aucune réponse n'est envoyée.
Adresse IP	Uniquement si **Réponse** = *Positif* Saisissez l'adresse IP qui est affectée pour **Nom d'hôte DNS**.
TTL	Saisissez la durée de validité de l'affectation de **Nom d'hôte DNS** à l'**Adresse IP** en secondes (important uniquement pour **Réponse** = *Positif*), qui sera transmise aux hôtes demandeurs. La valeur par défaut est *86400* (= 24 heures).

15.1.4 Extension de domaine

Le menu **Services locaux**->**DNS**->**Extension de domaine** contient la liste de toutes les transmissions configurées pour des domaines définis.

15.1.4.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres transmissions.

Le menu **Services locaux**->**DNS**->**Extension de domaine**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de transfert

Champ	Description
Transférer	Choisissez si un hôte ou un domaine doit être transmis. Valeurs possibles : • *Hôte* (valeur par défaut) • *Domaine*
Hôte	Uniquement pour **Transférer** = *Hôte* Saisissez le nom de l'hôte qui doit être transmis. L'entrée peut aussi débuter par un caractère de substitution,

Champ	Description
	par ex. *.bintec-elmeg.com. Lors de la saisie d'un nom sans point, le système le complète après confirmation par **OK** « **<Domaine par défaut.>** ». complété.
Domaine	Uniquement pour **Transférer** = *Domaine* Saisissez le nom du domaine qui doit être transmis. L'entrée peut aussi débuter par un caractère de substitution, par ex. *.bintec-elmeg.com. Lors de la saisie d'un nom sans point, le système le complète après confirmation par **OK** « **<Domaine par défaut.>** ». complété.
Transférer à	Choisissez où seront transmises les demandes au nom défini dans **Hôte** ou **Domaine**. Valeurs possibles : • *Interface* (valeur par défaut) : La demande est transmise à l'**Interface** définie. • *Serveur DNS*: La demande est transmise au **Serveur DNS** défini.
Interface	Uniquement pour **Transférer à** = *Interface* Choisissez l'interface via laquelle les demandes pour le **Domaine** défini doivent être reçues et transmises au serveur DNS.
Serveur DNS	Uniquement pour **Transférer à** = *Serveur DNS* Saisissez l'adresse IP du serveur DNS primaire et secondaire.

15.1.5 Cache

Le menu **Services locaux**->**DNS**->**Cache** affiche la liste de toutes les entrées de cache disponibles.

Vous pouvez sélectionner des entrées individuelles en cochant les cases correspondantes des différentes lignes, ou les sélectionner toutes à l'aide du bouton **Sélectionner tout**.

La sélection d'une entrée suivie de la confirmation par **Définir comme statique** entraîne

la conversion d'une entrée dynamique et une entrée statique. L'entrée correspondante disparait de cette liste et s'affiche dans la liste du menu **Hôtes statiques**. Le TTL est appliqué.

15.1.6 Statistiques

Le menu **Services locaux**->**DNS**->**Statistiques** affiche les valeurs statistiques suivantes :

Champs du menu Statistiques DNS

Champ	Description
Paquets DNS reçus	Permet d'afficher le nombre de paquets DNS reçus et transmis directement à votre appareil, y compris les paquets de réponses aux demandes transmises.
Paquet DNS invalide	Permet d'afficher le nombre de paquets DNS reçus invalides et adressés directement à votre appareil.
Requêtes DNS	Permet d'afficher le nombre de demandes DNS reçues valides et adressées directement à votre appareil.
Résultat cache	Permet d'afficher le nombre de demandes pour lesquelles une réponse à pu être générée à l'aide des entrées statiques ou des entrées dynamiques dans le cache.
Requêtes transférées	Permet d'afficher le nombre de demandes transmises à d'autres serveurs de noms.
Taux de résultat cache (%)	Permet d'afficher le nombre de **Résultat cache** par demande DNS en pour-cent.
Interrogations répondues avec succès	Permet d'afficher le nombre des demandes pour lesquelles une réponse (positive ou négative) a été envoyée.
Erreur de serveur	Permet d'afficher le nom de demandes auxquelles aucun serveur de noms n'a pu répondre (ni positivement, ni négativement).

15.2 HTTPS

Vous pouvez piloter l'interface utilisateur de votre appareil depuis n'importe quel PC avec navigateur Internet, même via une connexion HTTPS.

Le HTTPS (HyperText Transfer Protocol Secure) est alors le procédé pour établir une connexion cryptée et authentifiée SSL entre le navigateur utilisé pour la configuration et l'appareil.

15.2.1 Serveur HTTPS

Le menu **Services locaux**->**HTTPS**->**Serveur HTTPS** permet de configurer les paramètres de la connexion de configuration sécurisée par HTTPS.

Le menu **Services locaux**->**HTTPS**->**Serveur HTTPS** se compose des champs suivants :

Champs du menu Paramètres HTTPS

Champ	Description
Port HTTPS-TCP	Saisissez le port via lequel la connexion HTTPS doit être établie. Les valeurs possibles sont comprises entre *0* et *65535*. La valeur par défaut est *443*.
Certificat local	Sélectionnez un certificat à utiliser pour la connexion HTTPS. Valeurs possibles : • *Interne* (valeur par défaut) : Choisissez cette option si vous souhaitez utiliser le certificat prédéfini sur l'appareil. • *<Nom de certificat>* : Choisissez un certificat enregistré sous **Gestion du système**->**Certificats**->**Liste de certificat**.

15.3 Client DynDNS

L'utilisation d'adresses IP dynamiques présente l'inconvénient qu'un hôte du réseau ne peut plus être trouvé dès que son adresse IP change. DynDNS assure que votre appareil reste joignable même après un changement d'adresse IP.

Les étapes suivantes sont nécessaires pour la configuration :

- Enregistrement d'un nom d'hôte auprès d'un fournisseur d'accès DynDNS.
- Configuration de votre appareil

Enregistrement

Lors de l'enregistrement du nom d'hôte, vous définissez un nom d'utilisateur individuel

pour le service DynDNS, par ex. *dyn_client*. A cet effet, les fournisseurs d'accès proposent différents noms de domaines, de sorte à obtenir un nom d'hôte univoque pour votre appareil, par ex. *dyn_client.provider.com*. Le fournisseur d'accès DynDNS prend en charge la tâche de fournir à toutes les demandes DNS au sujet de l'hôte *dyn_client.provider.com* l'adresse IP dynamique de votre appareil comme réponse.

Afin que votre fournisseur d'accès soit toujour informé de l'adresse IP actuelle de votre appareil, votre appareil contacte lefournisseur d'accès à l'établissement d'une nouvelle connexion et propage son adresse IP actuelle.

15.3.1 Mise à jour DynDNS

Le menu **Services locaux**->**Client DynDNS**->**Mise à jour DynDNS** affiche la liste de tous les enregistrements DynDNS configurés qui doivent être actualisés.

15.3.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres enregistrements DynDNS actualisables.

Le menu **Services locaux**->**Client DynDNS**->**Mise à jour DynDNS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Nom de l'hôte	Saisissez le nom d'hôte complet tel qu'il est enregistré auprès du fournisseur d'accès DynDNS.
Interface	Sélectionnez l'interface WAN dont l'adresse IP doit être propagée via le service DynDNS (par ex. l'interface du fournisseur d'accès à Internet).
Nom de l'utilisateur	Saisissez le nom d'utilisateur tel qu'il est enregistré auprès du fournisseur d'accès DynDNS.
Mot de passe	Saisissez le mot de passe tel qu'il est enregistré auprès du fournisseur d'accès DynDNS.
Provider	Sélectionnez le fournisseur d'accès DynDNS auprès duquel les données ci-dessus sont enregistrées.

Champ	Description
	A l'état non configuré, vous disposez déjà d'un choix de fournisseurs d'accès DynDNS dont les protocoles sont supportés. D'autres fournisseurs d'accès DynDNS peuvent être configurés dans le menu **Services locaux**->**Client DynDNS**->**Fournisseur DynDNS**. La valeur par défaut est *DynDNS*.
Activer la mise à jour	Indiquez si l'entrée DynDNS configurée ici doit être activée. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Mail-Exchanger (MX)	Saisissez le nom d'hôte complet d'un serveur de messagerie vers lequel les e-mails doivent être transmis si l'hôte configuré ici ne doit pas recevoir d'e-mails. Renseignez-vous auprès de votre fournisseur d'accès au sujet de ce service de transmission et assurez-vous que les e-mails de l'hôte enregistré en tant que MX puissent être acceptés.
Wildcard	Choisissez si le transfert de tous les sous-domaines de **Nom de l'hôte** vers l'adresse IP actuelle de l'**Interface** doit être activé (résolution de nom étendue). Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

15.3.2 Fournisseur DynDNS

Le menu **Services locaux**->**Client DynDNS**->**Fournisseur DynDNS** affiche la liste de tous les fournisseurs d'accès DynDNS configurés.

15.3.2.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres fournisseurs d'accès DynDNS.

Le menu **Services locaux**->**Client DynDNS**->**Fournisseur DynDNS**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Nom du fournisseur	Saisissez un nom pour cette entrée.
Serveur	Saisissez le nom d'hôte ou l'adresse IP du serveur sur lequel est exécuté le service DynDNS du fournisseur d'accès.
Chemin de mise à jour	Indiquez le chemin d'accès sur le serveur du fournisseur d'accès, sur lequel se trouve le script pour la gestion de l'adresse IP de votre appareil. Renseignez-vous auprès de votre fournisseur d'accès au sujet du chemin d'accès à utiliser.
Port	Saisissez le port sur lequel votre appareil doit contacter le serveur de votre fournisseur d'accès. Renseignez-vous auprès de votre fournisseur d'accès au sujet du port correspondant. La valeur par défaut est *80*.
Journal	Sélectionnez l'un des protocoles implémentés. Valeurs possibles : • *DynDNS* (valeur par défaut) • *Static DynDNS* • *ODS* • *HN* • *DYNS* • *GnuDIP-HTML* • *GnuDIP-TCP* • *Custom DynDNS*

Champ	Description
	• *DnsExit*
Intervalle de mise à jour	Saisissez la durée (en secondes) que votre appareil doit attendre au minimum avant qu'il ne puisse propager une nouvelle fois sont adresse IP actuelle auprès du fournisseur d'accès DynDNS. La valeur par défaut est *300* secondes.

15.4 Serveur DHCP

Vous pouvez configurer votre appareil en tant que serveur DHCP (DHCP = Dynamic Host Configuration Protocol).

Chaque ordinateur dans votre réseau LAN requiert une adresse IP qui lui est propre. Cela s'applique aussi à votre appareil. Le protocole « Dynamic Host Configuration Protocol » (DHCP) vous permet d'affecter des adresses IP à votre réseau LAN. Si vous configurez votre appareil comme serveur DHCP, il attribue automatiquement des adresses IP provenant d'un pool d'adresses IP défini à des ordinateurs demandeurs du réseau LAN.

Lorsqu'un client requiert pour la première fois une adresse IP, il envoie une demande DHCP (avec son adresse MAC) comme diffusion de réseau aux serveurs DNCP disponibles. Le client reçoit alors (dans le cadre d'une brève communication) sont adresse IP du bintec elmeg.

Ainsi, vous n'avez pas besoin d'affecter des adresses IP fixes aux ordinateurs et la complexité de la configuration de votre réseau diminue. A cet effet, vous devez configurer un pool d'adresses IP depuis lequel votre appareil attribue des adresses IP aux hôtes du réseau LAN, et ce pour des durées définies. Un serveur DHCP transmet aussi les adresses du serveur de nom de domaine (DNS) enregistré statiquement ou par négociation PPP, du serveur de nom NetBIOS (WINS) et de la passerelle par défaut.

15.4.1 Configuration pool d'adresses IP

Le menu **Services locaux**->**Serveur DHCP**->**Configuration pool d'adresses IP** affiche la liste de tous les pools d'IP configurés. Cette liste est globale et affiche aussi les pools configurés dans d'autres menus.

15.4.1.1 Editer ou Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres pools d'adresses IP. Sélectionnez le symbole pour traiter les entrées existantes.

Champs du menu Paramètres de base

Champ	Description
Nom de pool IP	Saisissez une description pour désigner clairement le pool d'adresses IP.
Plage d'adresses IP	Saisissez la première (premier champ) et la dernière (deuxième champ) adresse IP du pool d'adresses IP.
Serveur DNS	**Primaire** : saisissez l'adresse IP du serveur DNS qui doit être utilisé de préférence par les clients qui reçoivent une adresse issue de ce pool d'adresses. **Secondaire** : saisissez l'adresse IP d'un autre serveur DNS.

15.4.2 Configuration DHCP

Pour activer votre appareil comme serveur DHCP, vous devez d'abord définir le pool d'adresses IP depuis lequel les adresses IP sont distribuées aux clients demandeurs.

Le menu **Services locaux**->**Serveur DHCP**->**Configuration DHCP** affiche la liste de tous les pools d'adresses IP configurés.

Pour chaque entrée, la liste permet d'activer ou de désactiver les pools DHCP créés sous **État**.

Note

A la livraison, le pool DHCP est préconfiguré avec les adresses IP 192.168.0.10 à 192.168.0.49. Il est utilisé si aucun autre serveur DHCP n'est disponible dans le réseau.

15.4.2.1 Editer ou Nouveau

Sélectionnez le bouton **Nouveau** pour configurer d'autres pools d'adresses IP. Sélectionnez le symbole pour traiter les entrées existantes.

Le menu **Services locaux**->**Serveur DHCP**->**Configuration DHCP**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Interface	Sélectionnez l'interface via laquelle les adresses définies dans la **Plage d'adresses IP** sont attribuées à des clients DHCP demandeurs. Si une demande DHCP est reçue via cette **Interface**, une des adresses du pool d'adresses est attribuée.
Nom de pool IP	Saisissez une description pour désigner clairement le pool d'adresses IP.
Utilisation pool	Choisissez si le pool IP doit être utilisé pour les demandes DHCP dans le même sous-réseau ou pour les demandes DHCP transmises depuis un autre sous-réseau vers votre appareil. Dans ce cas, il est possible de définir des adresses IP d'un autre réseau. Valeurs possibles : • *Local* (valeur par défaut) : Le pool DHCP n'est utilisé que pour les demandes DHCP provenant du même sous-réseau. • *Relais*: Le pool DHCP n'est utilisé que pour les demandes DHCP transmises depuis un autre sous-réseau. • *Local/Relais*: Le pool DHCP est utilisé pour les demandes DHCP du même sous-réseau et provenant d'autres sous-réseaux.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Passerelle	Choisissez l'adresse IP diot être transmise au client DHCP comme passerelle. Valeurs possibles : • *Utiliser le routeur comme passerelle* (valeur par défaut) : Ici est transmise l'adresse IP définie pour l'**Interface**. • *Pas de passerelle*: Aucune adresse IP n'est transmise. • *Spécifier*: Saisissez l'adresse IP correspondante.
Lease Time	Indiquez la durée (en minutes) pendant laquelle une adresse

Champ	Description
	du pool doit être affectée à un hôte. Après écoulement du **Lease Time**, l'adresse peut être réaffectée par le serveur. La valeur par défaut est *120*.
Options DHCP	Indiquez les données supplémentaires devant être transmises au client DHCP. Valeurs possibles pour **Option** : • *Serveur horaire* (valeur par défaut) : Saisissez l'adresse IP du serveur horaire qui doit être transmise au client. • *Serveur DNS*: Saisissez l'adresse IP du serveur DNS qui doit être transmise au client. • *Nom de domaine DNS*: Saisissez le domaine DNS qui doit être transmis au client. • *Serveur WINS/NBNS*: Saisissez l'adresse IP du serveur WINS/NBNS qui doit être transmise au client. • *Type de noeud WINS/NBT*: Saisissez le type du nœud WINS/NBT qui doit être transmis au client. • *Serveur TFTP*: Saisissez l'adresse IP du serveur TFTP qui doit être transmise au client. • *Contrôleur CAPWAP*: Saisissez l'adresse IP du contrôleur CAPWAY qui doit être transmise au client. • *URL (serveur de provisioning)* : Cette option vous permet de transmettre une URL quelconque à un client. Utilisez cette option pour transmettre aux téléphones IP demandeurs l'URL du serveur de provisioning si un provisioning automatique des téléphones doit être réalisé. L'URL doit alors se présenter sous la forme *http://<IP-Adresse des Provisionierungsservers>/eg_prov*. • *Groupe de fabricants* (Vendor Specific Information) : Cette option vous permet de transmettre au client des informations spécifiques au fabricant dans une chaîne de caractères de texte quelconque. Plusieurs entrées sont possibles. Ajoutez d'autres entrées à l'aide du bouton **Ajouter**.

Editer

Im Menü **Services locaux** ->**Serveur DHCP** ->**Configuration DHCP**->**Paramètres étendus** vous permet d'éditer une entrée dans le champ **Options DHCP** si **Option** = *Groupe de fabricants* est sélectionné.

Sélectionnez le symbole pour éditer une entrée existante. Dans le menu en superposition, vous pouvez configurer les réglages du serveur DHCP spécifiques au fabricant pour les adapter à certains téléphones.

Champs du menu Paramètres de base

Champ	Description
Sélectionner fournisseur	Ce paramètre n'est actuellement pas utilisé par votre appareil. Ici, vous pouvez choisir les valeurs spécifiques au fabricant qui seront transmises pour le serveur DHCP. Valeurs possibles : • *Siemens* (valeur par défaut) • *Divers*
Provisioning-Server (code 3)	Ce paramètre n'est actuellement pas utilisé par votre appareil. Indiquez la valeur spécifique au fabricant qui doit être transmise. Pour le réglage **Sélectionner fournisseur** = *Siemens*, la valeur par défaut *sdlp* s'affiche. Vous pouvez compléter l'adresse IP du serveur souhaité.

15.4.3 Liaison IP/MAC

Le menu **Services locaux**->**Serveur DHCP**->**Liaison IP/MAC** affiche une liste de tous les clients qui ont reçus une adresse IP par DHCP de votre appareil.

Vous pouvez affecter à certaines adresses MAC une adresse IP souhaitée d'un pool d'adresses IP défini. A cet effet, vous pouvez sélectionner l'option **Liaison statique** dans la liste pour appliquer une entrée de liste comme lien fixe, ou définir manuellement une liaison IP/MAC fixe en la configurant dans le sous-menu **Nouveau**.

Note

Les nouvelles liaisons IP/MAC statiques ne peuvent être créées que lorsque les plages d'adresse IP ont été définies dans **Services locaux**->**Serveur DHCP**->**Configuration DHCP**.

15.4.3.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres liaisons IP/MAC.

Le menu **Services locaux**->**Serveur DHCP**->**Liaison IP/MAC**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez le nom de l'hôte pour lequel l'**Adresse MAC** est liée à l'**Adresse IP**. Une chaîne peut contenir 256 caractères maximum.
Adresse IP	Saisissez l'adresse IP qui doit être affectée à l'adresse MAC indiquée dans **Adresse MAC**.
Adresse MAC	Saisissez l'adresse MQC qui doit être affectée à l'adresse IP indiquée dans **Adresse IP**.

15.4.4 Paramètres DHCP-Relay

Si votre adresse ne distribue pas d'adresse IP par DHCP aux clients du réseau local, il peut néanmoins transmettre les demandes DHCP du réseau local vers un serveur DHCP distant. Le serveur DHCP attribue à votre appareil une adresse IP de son pool, et celui-ci l'envoie au client dans le réseau local.

Le menu **Services locaux**->**Serveur DHCP**->**Paramètres DHCP-Relay** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Serveur DHCP pri-	Saisissez l'adresse IP d'un serveur auquel les demandes de

Champ	Description
maire	BootP ou DHCP doivent être transmises.
Serveur DHCP secondaire	Saisissez l'adresse IP d'un serveur BootP ou DHCP alternatif.

15.5 Serveur CAPI

La fonction de serveur CAPI vous permet d'attribuer des noms d'utilisateurs et des mots de passe aux utilisateurs des applications CAPI de votre appareil. Ainsi, vous pouvez assurer que seuls des utilisateurs autorisés puissent réceptionner les appels entrants et établir des connexions sortantes via CAPI.

Le service CAPI permet aux appels de données et vocaux entrants et sortants de se connecter aux applications de communication sur des hôtes du réseau LAN qui accèdent à l'interface CAPI distance de votre appareil. Ainsi, des hôtes connectés à votre appareil peuvent par exemple recevoir et envoyer des fax.

Note

Tous les appels entrants vers CAPI sont proposés à toutes les applications CAPI enregistrées et « à l'écoute ».

A la livraison, un utilisateur avec le nom d'utilisateur *default* et sans mot de passe est enregistré pour le sous-système CAPI.

Lorsque vous aurez créé vos utilisateurs souhaités avec leurs mot de passe, vous devrez supprimer l'utilisateur *default* dans mot de passe.

15.5.1 Utilisateur

Le menu **Services locaux**->**Serveur CAPI**->**Utilisateur** affiche la liste de tous les utilisateurs CAPI configurés.

15.5.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres utilisateurs CAPI.

Le menu **Services locaux**->**Serveur CAPI**->**Utilisateur**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Nom de l'utilisateur	Saisissez le nom d'utilisateur pour lequel l'accès au service CAPI doit être autorisé ou bloqué.
Mot de passe	Saisissez le mot de passe avec lequel l'utilisateur **Nom de l'utilisateur** doit s'identifier pour pouvoir accéder au service CAPI.
Accès	Choisissez si l'accès au service CAPI doit être autorisé ou bloqué pour l'utilisateur. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.

15.5.2 Options

Le menu **Services locaux**->**Serveur CAPI**->**Options** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Activer le serveur	Indiquez si votre appareil doit être activé en tant que serveur CAPI. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
En-tête de télécopie	Uniquement pour les appareils de la gamme **RTxxx2** Choisissez si l'en-tête de fax doit être imprimé sur le bord supérieur de la page des fax sortants. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Port TCP du serveur CAPI	Le champ ne peut être édité que lorsque **Activer le serveur** est activé. Saisissez le numéro de port TCP pour les connexions CAPI

Champ	Description
	distantes. La valeur par défaut est *2662*.

15.6 Scheduling

Votre appareil est équipé d'un planning de tâches qui permet de réaliser certaines actions standard (par ex. l'activation ou la désactivation d'interfaces). De plus, chaque variable MIB existante est configurable avec n'importe quelle valeur.

Définissez les **Actions** souhaitées, ainsi que les **Déclencheur** qui décident quand et sous quelles conditions les **Actions** sont exécutées. Un **Déclencheur** peut être un événement unique ou une séquence d'événements regroupés dans une **Liste des événements**. Pour un événement unique, vous devez également créer une liste d'événements, qui ne contiendra cependant qu'un seul événement.

Il est possible de déclencher des actions en fonction d'une durée. De plus, le statut ou la joignabilité des interfaces ou leur trafic de données peut conduire à l'exécution des actions configurées, mais aussi la validité des licences. Ici aussi, il est possible de configurer une variable MIB quelconque avec une valeur quelconque comme déclencheur.

Pour la mise en service du planning des tâches, il convient d'activer l'**Intervalle Schedule** sous **Options**. Cet intervalle défini l'écart temporel selon lequel le système vérifie si au moins un événement est survenu. Cet événement sert de déclencheur pour une action configurée.

Attention

La configuration des actions non prédéfinies requiert des connaissances étendues au sujet du mode de fonctionnent des passerelles **Gigaset**. Une configuration erronée peut entraîner des perturbations importantes de fonctionnement. Le cas échéant, sauvegardez la configuration d'origine, p. ex., sur votre PC.

Note

La condition première pour le fonctionnement du planning des tâches est une date postérieure au 01/01/2000 réglée sur votre ordinateur.

15.6.1 Déclencheur

Le menu **Services locaux**->**Scheduling**->**Déclencheur** affiche toutes les listes d'événements configurées. Chaque liste d'événements contient au moins un événement prévu comme déclencheur pour une action.

15.6.1.1 Nouveau

Actionnez le bouton **Nouveau** pour créer d'autres listes d'événements supplémentaires.

Le menu **Services locaux**->**Scheduling**->**Déclencheur**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Liste des événements	L'option *Nouveau* (valeur par défaut) vous permet de créer une nouvelle liste d'événements. L'option **Description** vous permet d'affecter un nom à cette liste. Les autres paramètres vous permettent de créer le premier événement de la liste. Si vous souhaitez compléter une liste d'événements existante, vous devez sélectionner la liste d'événements souhaitée et y ajouter un moins un événement. Les listes d'événements servent aussi à créer des conditions complexes pour le déclenchement d'une action. Les événements sont exécutés dans l'ordre dans lequel ils figurant dans la liste.
Description	Uniquement pour **Liste des événements** = *Nouveau* Saisissez une désignation quelconque pour la liste d'événements.
Type d'événement	Sélectionnez le type d'événement. Valeurs possibles : • *Heure* (valeur par défaut) : Les actions configurées et affectées dans **Actions** sont déclenchées à des moments précis. • *MIB/SNMP*: Les actions configurées et affectées dans **Actions** sont déclenchées lorsque les variables MLIB définis adoptent les valeurs indiquées.

Champ	Description
	• *Etat de l'interface*: Les actions configurées et affectées dans **Actions** sont déclenchées lorsque les interfaces définies adoptent un statut spécifique. • *Trafic interface*: Les actions configurées et affectées dans **Actions** sont déclenchées lorsque le trafic de données sur les interfaces indiquées dépasse positivement ou négativement la valeur définie. • *Test Ping*: Les actions configurées et affectées dans **Actions** sont déclenchées lorsque l'adresse IP indiquée est joignable ou n'est pas joignable. • *Durée de vie d'un certificat*: Les actions configurées et affectées dans **Actions** sont déclenchées lorsque la durée de validité définie est atteinte. • *État zone GEO* :Les actions configurées et affectées dans **Actions** sont déclenchées lorsque les **Zones GEO** définies adoptent un statut spécifique.
Zone GEO contrôlée	Uniquement pour **Type d'événement** *État zone GEO* Sélectionnez une zone GEO configurée.
Etat de la zone GEO	Uniquement pour **Type d'événement** *État zone GEO* Sélectionnez l'**Etat de zone GEO**. Valeurs possibles : • *Vrai*: La position actuelle se trouve à l'intérieur de la zone définie. • *Faux*: La position actuelle se trouve à l'extérieur de la zone définie.
Variable surveillée	Uniquement pour **Type d'événement** *MIB/SNMP* Sélectionnez la variable MIB dont la valeur définie doit être configurée comme déclencheur. Sélectionnez d'abord le **Système** sur lequel la variable MIB est enregistrée, puis le **Tableau MIB** et enfin la **Variable MIB** elle-même. Seuls les tableaux et variables MIB disponibles dans la zone respective s'affichent.
Condition de comparaison	Uniquement pour **Type d'événement** *MIB/SNMP*

Champ	Description
	Choisissez si la variable doit être *Plus grand* (valeur par défaut), *Egal*, *Inférieur* ou être *Différent* de la valeur indiquée dans *Valeur de comparaison* ou doit se situer au sein de la *Plage*pour déclencher l'action.
Valeur de comparaison	Uniquement pour **Type d'événement** *MIB/SNMP* Saisissez la valeur de la variable MIB.
Variables d'index	Uniquement pour **Type d'événement** *MIB/SNMP* Le cas échéant, sélectionnez des variables MIB pour identifier sans équivoque un jeu de données spécifique du **Tableau MIB**, par ex. *ConnIfIndex*. La combinaison de **Variable d'index** (en principe, une variable d'index indiquée par *) et **Valeur d'index** débouche sur une identification claire d'une entrée spécifique du tableau. Créez d'autres **Variables d'index** à l'aide de **Ajouter**.
Interface surveillée	Uniquement pour **Type d'événement** *Etat de l'interface* et *Trafic interface* Sélectionnez l'interface dont l'état défini doit déclencher un événement.
Etat de l'interface	Uniquement pour **Type d'événement** *Etat de l'interface* Sélectionnez l'état que l'interface doit adpoter pour déclencher l'action souhaitée. Valeurs possibles : • *Actif* (valeur par défaut) : L'interface est active. • *Inactif*: L'interface est inactive.
Sens de l'échange de données	Uniquement pour **Type d'événement** *Trafic interface* Sélectionnez le sens du trafic de données dont les valeurs doivent être observées pour le déclenchement d'une action. Valeurs possibles : • *RX* (valeur par défaut) : Le trafic de données entrant est sur-

Champ	Description
	veillé. • *TX*: Le trafic de données sortant est surveillé.
Condition de trafic de l'interface	Uniquement pour **Type d'événement** *Trafic interface* Choisissez si la valeur pour le trafic de données doit être *Plus grand* (valeur par défaut) ou *Inférieur* à la valeur indiquée dans *Echange de données transmis* pour déclencher l'action.
Echange de données transmis	Uniquement pour **Type d'événement** *Trafic interface* Saisissez dans **koctets** la valeur souhaitée pour le trafic de données de comparaison. La valeur par défaut est *0*.
Adresse IP de destination	Uniquement pour **Type d'événement** *Test Ping* Saisissez l'adresse IP dont l'accessibilité doit être vérifiée.
Adresse IP source	Uniquement pour **Type d'événement** *Test Ping* Saisissez l'adresse IP à utiliser comme adresse d'expédition pour le test Ping. Valeurs possibles : • *Automatique* (valeur par défaut) : L'adresse IP de l'interface via laquelle le Ping est envoyé est automatiquement entrée en tant qu'adresse d'expédition. • *Spécifique*: saisissez l'adresse IP de votre choix dans la zone de texte.
État	Uniquement pour **Type d'événement** *Test Ping* Choisissez si l'**Adresse IP de destination** doit être *Accessible* (valeur par défaut) ou *Non accessible* pour déclencher l'action.
Intervalle	Uniquement pour **Type d'événement** *Test Ping* Saisissez le délai en **Secondes**, à l'issue duquel un Ping doit de nouveau être envoyé.

Champ	Description
	La valeur par défaut est *60* secondes.
Tentatives	Uniquement pour **Type d'événement** *Test Ping* Saisissez le nombre de tests de Ping à réaliser jusqu'à ce que l'**Adresse IP de destination** est considérée comme *Non accessible*. La valeur par défaut est *3*.
Certificat surveillé	Uniquement pour **Type d'événement** *Durée de vie d'un certificat* Sélectionnez le certificat dont la validité doit être contrôlée.
Durée de validité restante	Uniquement pour **Type d'événement** *Durée de vie d'un certificat* Saisissez la valeur souhaitée pour la validité restante du certificat en pour-cent.

Champs du menu Sélectionner l'intervalle de temps

Champ	Description
Condition horaire	Uniquement pour **Type d'événement** *Temps* Sélectionnez d'abord le type d'indication de temps dans **Type de condition**. Valeurs possibles : • *Jour de la semaine*: Sélectionnez un jour de la semaine dans **Paramètres de condition**. • *Périodes* (valeur par défaut) : Sélectionnez un cycle spécifique dans **Paramètres de condition**. • *Jour du mois*: Sélectionnez un jour spécifique du mois dans **Paramètres de condition**. Valeurs possibles pour **Paramètres de condition** si **Type de condition** = *Jour de la semaine* : *Lundi* (valeur par défaut) ... *Dimanche*. Valeurs possibles pour **Paramètres de condition** si **Type de**

Champ	Description
	condition = *Périodes* : • *Quotidien*: Le déclencher est activé quotidiennement (valeur par défaut) • *Lundi-Vendredi*: Le déclencher est activé du lundi au vendredi. • *Lundi-Samedi* : Le déclencher est activé du lundi au samedi. • *Samedi-Dimanche* : Le déclencheur est activé le samedi et le dimanche. Valeurs possibles pour **Paramètres de condition** si **Type de condition** = *Jour du mois* : *1*... *31*.
Heure de début	Saisissez le moment d'activation du déclencheur. L'activation est réalisée avec le prochain intervalle de planning. La valeur par défaut de cet intervalle est de 55 secondes.
Temps d'arrêt	Saisissez le moment de désactivation du déclencheur. La désactivation est réalisée avec le prochain intervalle de planning. Si vous n'indiquez pas d'**Temps d'arrêt** ou activez **Temps d'arrêt** = **Heure de début**, le déclencheur est activé et désactivé après 10 secondes.

15.6.2 Actions

Le menu **Services locaux**->**Scheduling**->**Actions** affiche la liste de toutes les actions qui doivent être déclenchées par les événements ou chaînes d'événements configurées dans **Services locaux**->**Scheduling**->**Déclencheur**.

15.6.2.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres actions supplémentaires.

Le menu **Services locaux**->**Scheduling**->**Actions**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez une désignation quelconque pour l'action.
Type d'instruction	Sélectionnez l'action souhaitée. Valeurs possibles : • *Redémarrage* (valeur par défaut) : Votre appareil est redémarré. • *MIB/SNMP*: La valeur souhaitée est saisie pour une variable MIB. • *Etat de l'interface*: L'état d'une interface est modifiée. • *État WLAN*: uniquement pour les appareils avec Wireless LAN. L'état d'un SSID WLAN est modifié. • *Mise à jour du logiciel*: Une mise à jour de logiciel est initiée. • *Gestion de la configuration*: Un fichier de configuration est chargé dans votre appareil ou sauvegardé depuis votre appareil. • *Test Ping*: La joignabilité d'une adresse IP est contrôlée. • *Gestion des certificats*: Un certificat doit être renouvelé, supprimé ou enregistré. • *5 GHz-WLAN-Bandscan*: uniquement pour les appareils avec Wireless LAN. Un scan de la bande de fréquences 5 GHz est effectué. • *5,8 GHz-WLAN-Bandscan*: uniquement pour les appareils avec Wireless LAN. Un scan de la bande de fréquences 5,8 GHz est effectué. • *WLC : nouveau scan Neighbor*: Uniquement pour les appareils avec contrôleur WLAN. Un scan voisin est déclenché dans un réseau WLAN contrôlé par le contrôleur WLAN. • *WLC : État VSS*: Uniquement pour les appareils avec contrôleur WLAN. L'état d'un réseau sans fil est modifié. • *WLAN : Mode d'opération*: Le mode de fonctionnement d'un module radio WLAN est modifié.
Liste des événements	Sélectionnez la liste d'événements souhaitée créée dans **Services locaux**->**Scheduling**->**Déclencheur**.
Condition pour la liste d'événements	Dans la liste d'événements sélectionnée, choisissez le nombre

Champ	Description
	d'événement configurés qui doivent se produire afin de déclencher l'action. Valeurs possibles : • *Tous* (valeur par défaut) : L'action est déclenchée lorsque toutes les événements se produisent. • *Un*: L'action est déclenchée lorsqu'un événement se produit. • *aucun*: L'action est déclenchée lorsqu'aucun des événements se produit. • *Non un*: L'action est déclenchée lorsqu'un des événements ne se produit pas.
Redémarrage de l'appareil après	Uniquement si **Type d'instruction** = *Redémarrage* Saisissez la durée en secondes, pendant laquelle la survenue de l'événement doit être attendue avant de redémarrer l'appareil. La valeur par défaut est *60* secondes.
Variables MIB/SNMP à ajouter/à éditer	Uniquement si **Type d'instruction** = *MIB/SNMP* Sélectionnez le tableau MIB dans lequel est enregistrée la variable MIB dont la valeur doit être modifiée. Sélectionnez d'abord le **Système**, puis le **Tableau MIB**. Seuls les tableaux MIB disponibles dans la zone respective s'affichent.
Mode d'instruction	Uniquement si **Type d'instruction** = *MIB/SNMP* Choisissez comment manipuler l'entrée MIB. Sont disponibles : • *Modifier l'entrée existante* (valeur par défaut) : Une entrée existante doit être modifiée. • *Créer une nouvelle entrée MIB*: Une nouvelle entrée doit être créée.
Variables d'index	Uniquement si **Type d'instruction** = *MIB/SNMP* Le cas échéant, sélectionnez des variables MIB pour identifier sans équivoque un jeu de données spécifique du **Tableau**

Champ	Description
	, par ex. *ConnIfIndex*. La combinaison de **Variable d'index** (en principe, une variable d'index indiquée par *) et **Valeur d'index** débouche sur une identification claire d'une entrée spécifique du tableau. Créez d'autres **Variables d'index** à l'aide de **Ajouter**.
État du déclencheur	Uniquement si **Type d'instruction** = *MIB/SNMP* Sélectionnez l'état que doit présenter l'événement pour modifier la variable MIB conformément à la définition. Valeurs possibles : • *Actif* (valeur par défaut) : La valeur de la variable MIB est modifiée si le déclencheur est actif. • *Inactif*: La valeur de la variable MIB est modifiée si le déclencheur est inactif. • *Les deux*: La valeur de la variable MIB est modifiée de manière différente si l'état du déclencheur change.
Variables MIB	Uniquement si **Type d'instruction** = *MIB/SNMP* Sélectionnez la variable MIB dont la valeur doit être modifiée en fonction de l'état du déclencheur. Si le déclencheur est actif (**État du déclencheur** *Actif*), la variable MIB est complétée avec la valeur saisie dans **Valeur active.**. Si le déclencheur est inactif (**État du déclencheur** *Inactif*), la variable MIB est complétée avec la valeur saisie dans **Valeur inactive**. Si la variable MIB doit être modifiée en fonction de l'état actif ou inactif du déclencheur (**État du déclencheur** *Les deux*), elle est complétée pour un déclencheur actif avec la valeur saisie dans **Valeur active.** et pour un déclencheur inactif avec la valeur saisie dans **Valeur inactive**. Créez d'autres entrées avec **Ajouter**.
Interface	Uniquement si **Type d'instruction** = *Etat de l'interface* Sélectionnez l'interface dont l'état doit être modifié.

Champ	Description
Définir l'état de l'interface	Uniquement si **Type d'instruction** = *Etat de l'interface* Sélectionnez l'état sur lequel l'interface doit être commuté. Valeurs possibles : • *Actif* (valeur par défaut) • *Inactif* • *Réinitialiser*
WLAN-SSID local	Uniquement si **Type d'instruction** = *État WLAN* Sélectionnez le réseau sans fil souhaité dont l'état doit être modifié.
Définir l'état	Uniquement si **Type d'instruction** = *État WLAN* Sélectionnez l'état que le réseau sans fil doit obtenir. Valeurs possibles : • *Activer* (valeur par défaut) • *Désactiver*
Source	Uniquement si **Type d'instruction** = *Mise à jour du logiciel* Sélectionnez la source souhaitée pour la mise à jour du logiciel. Valeurs possibles : • *Logiciel en cours du serveur de mise à jour* (valeur par défaut) : Le logiciel actuel est chargé depuis le serveur de mise à jour. • *Serveur HTTP*: Le logiciel actuel est chargé depuis un serveur HTTP que vous définissez à l'aide de l' *URL du serveur*. • *Serveur HTTPS*: Le logiciel actuel est chargé depuis un serveur HTTPS que vous définissez à l'aide de l' *URL du serveur*. • *Serveur TFTP*: Le logiciel actuel est chargé depuis un serveur TFTP que vous définissez à l'aide de l' *URL du ser-*

Champ	Description
	veur.
URL du serveur	Pour **Type d'instruction** = *Mise à jour du logiciel* si **Source** non *Logiciel en cours du serveur de mise à jour* Saisissez l'URL du serveur depuis lequel vous souhaitez charger la version souhaitée du logiciel. Pour **Type d'instruction** = *Gestion de la configuration* avec **Action** = *Importer la configuration* ou *Exporter la configuration* Saisissez l'URL du serveur depuis lequel un fichier de configuration doit être chargé ou sur lequel le fichier de configuration doit être sauvegardé.
Nom du fichier	Si **Type d'instruction** = *Mise à jour du logiciel* Saisissez le nom de fichier de la version du logiciel. Pour **Type d'instruction** = *Gestion des certificats* avec **Action** = *Importer le certificat* Saisissez le nom de fichier du fichier de certificat.
Action	Si **Type d'instruction** = *Gestion de la configuration* Sélectionnez l'action qui doit être appliquée à un fichier de configuration. Valeurs possibles : • *Importer la configuration* (valeur par défaut) • *Exporter la configuration* • *Renommer la configuration* • *Supprimer la configuration* • *Copier la configuration* Si **Type d'instruction** = *Gestion des certificats* Sélectionnez l'action que vous souhaitez appliquer à un fichier de certificat. Valeurs possibles :

Champ	Description
	• *Importer le certificat* (valeur par défaut) • *Supprimer le certificat* • *SCEP*
Journal	Uniquement pour **Type d'instruction** = *Gestion des certificats* et *Gestion de la configuration* si **Action** = *Importer la configuration* Sélectionnez le protocole pour la transmission des données. Valeurs possibles : • *HTTP* (valeur par défaut) • *HTTPS* • *TFTP*
Format de fichier CSV	Uniquement si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Importer la configuration* ou *Exporter la configuration* Indiquez si le fichier doit être transmis au format CSV. Le format CSV peut être lu et modifié sans problèmes. Vous pouvez en outre afficher les données correspondantes sous la forme d'un aperçu, p. ex. à l'aide de Microsoft Excel. La fonction est activée par défaut.
Nom du fichier sur le serveur	Uniquement si **Type d'instruction** = *Gestion de la configuration* Pour **Action** = *Importer la configuration* Saisissez le nom du fichier sous lequel il est enregistré sur le serveur depuis lequel il doit être chargé. Pour **Action** = *Exporter la configuration* Saisissez le nom du fichier sous lequel il doit être enregistré sur le serveur.
Nom de fichier local	Uniquement si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Importer la configuration*, *Renommer la configuration* ou *Copier la*

Champ	Description
	configuration Pour l'importer, le renommer ou le copier, saisissez un nom pour le fichier de configuration sous lequel il doit être enregistré localement sur l'appareil.
Nom du fichier dans flash	Si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Exporter la configuration* Sélectionnez le fichier à exporter. Si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Renommer la configuration* Sélectionnez le fichier à renommer. Si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Supprimer la configuration* Sélectionnez le fichier à supprimer. Si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Copier la configuration* Sélectionnez le fichier à copier.
La configuration contient des certificats/clés	Uniquement si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Importer la configuration* ou *Exporter la configuration* Choisissez si les certificats et codes contenus dans la configuration doivent être exportés ou importés. La fonction est désactivée par défaut.
Crypter la configuration	Uniquement si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Importer la configuration* ou *Exporter la configuration* Indiquez si les données de l'**Action** sélectionnée doivent être cryptées. La fonction est désactivée par défaut.

Champ	Description
Redémarrer après exécution de la commande	Uniquement si **Type d'instruction** = *Gestion de la configuration* Choisissez si votre appareil doit être redémarré après l'**Action** souhaitée. La fonction est désactivée par défaut.
Contrôle de la version	Uniquement si **Type d'instruction** = *Gestion de la configuration* et **Action** = *Importer la configuration* Choisissez si lors de l'importation d'un fichier de configuration, il sera vérifié si une version plus récente de la configuration chargée est déjà disponible sur le serveur. Dans le cas contraire, l'importation du fichier est annulée. La fonction est désactivée par défaut.
Adresse IP de destination	Uniquement si **Type d'instruction** = *Test Ping* Saisissez l'adresse IP dont l'accessibilité doit être vérifiée.
Adresse IP source	Uniquement si **Type d'instruction** = *Test Ping* Saisissez l'adresse IP à utiliser comme adresse d'expédition pour le test Ping. Valeurs possibles : • *Automatique* (valeur par défaut) : L'adresse IP de l'interface via laquelle le Ping est envoyé est automatiquement entrée en tant qu'adresse d'expédition. • *Spécifique*: saisissez l'adresse IP de votre choix dans la zone de texte.
Intervalle	Uniquement si **Type d'instruction** = *Test Ping* Saisissez le délai en **Secondes**, à l'issue duquel un Ping doit de nouveau être envoyé. La valeur par défaut est de *1* secondes.
Tentatives	Uniquement si **Type d'instruction** = *Test Ping*

Champ	Description
	Saisissez le nombre de tests de Ping à réaliser jusqu'à ce que l'**Adresse IP de destination** est considérée comme non joignable. La valeur par défaut est *3*.
Adresse du serveur	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *Importer le certificat* Saisissez l'URL du serveur depuis lequel vous souhaitez charger un ficheir de certificat.
Description de certificat locale	Si **Type d'instruction** = *Gestion des certificats* et **Action** = *Importer le certificat* Saisissez une description pour le certificat, sous laquelle il sera enregistré sur l'appareil. Si **Type d'instruction** = *Gestion des certificats* et **Action** = *Supprimer le certificat* Sélectionnez le certificat à supprimer.
Mot de passe pour certificat protégé	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *Importer le certificat* Choisissez si vous souhaitez utiliser un certificat protégé qui requiert un mot de passe, et saisissez celui-ci dans le champ de saisie. La fonction est désactivée par défaut.
Ecraser certificat similaire	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *Importer le certificat* Choisissez si vous souhaitez écraser un certificat déjà disponible sur votre appareil par le nouveau certificat. La fonction est désactivée par défaut.
Ecrire le certificat dans la configuration	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *Importer le certificat* Choisissez si vous souhaitez intégrer le certificat dans un fichier de configuration et sélectionnez le fichier de configuration

Champ	Description
	souhaité. La fonction est désactivée par défaut.
Description de la demande de certificat	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Saisissez une description sous laquelle le certificat SCEP doit être enregistré sur votre appareil.
URL serveur SCEP	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Saisissez l'URL du serveur SCEP, par ex. *http://scep.bintec-elmeg.com:8080/scep/scep.dll* Les données correspondantes vous sont transmises par votre administrateur CA.
Nom de l'objet	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Saisissez le nom de sujet avec les attributs. Exemple : *« CN=VPNServer, DC=mydomain, DC=com, c=DE »*
Nom CA	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Saisissez le nom du certificat CA de l'organisme de certification (CA) auprès duquel vous souhaitez soumettre cotre demande de certificat, par ex. *cawindows*. Les données correspondantes vous sont transmises par votre administrateur CA.
Mot de passe	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Pour obtenir des certificats, vous aurez éventuellement besoin d'un mot de passe attribué par l'organisme de certification. Saisissez ici le mot de passe qui vous a été octroyé par votre organisme de certification.

Champ	Description
Taille de la clé	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Choisissez la longueur du code à générer. Les valeurs possibles sont *1024* (valeur par défaut), *2048* et *4096*.
Mode enregistrement automatique	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Indiquez si votre appareil enregistre automatiquement en interne les différentes étapes du processus d'enregistrement. Ceci est utile lorsque l'enregistrement ne peut pas être terminé tout de suite. Si l'état n'a pas été enregistré, l'enregistrement incomplet ne peut pas être terminé. Dès que l'enregistrement est terminé et que le certificat a été téléchargé depuis le serveur CA, il est automatiquement enregistré dans la configuration de votre appareil. La fonction est activée par défaut.
Utiliser CRL	Uniquement si **Type d'instruction** = *Gestion des certificats* et **Action** = *SCEP* Définissez ici dans quelle mesure les listes de blocage (CRL) doivent être incluses dans la validation des certificats émis par leurs propriétaires. Valeurs possibles : • *Auto* (valeur par défaut) : Si le certificat CA inclut une entrée pour un point de distribution de listes de blocage de certificats (CDP, CRL Distribution Point), celle-ci doit être analysée en plus des listes de blocage configurées globalement dans l'appareil. • *Oui*: les CRL sont vérifiées de manière approfondie. • *Non*: Pas de vérification des CRL.

15.6.3 Options

Le menu **Services locaux**->**Scheduling**->**Options** permet de configurer l'intervalle de planification.

Le menu **Services locaux**->**Scheduling**->**Options** se compose des champs suivants :

Champs du menu Options scheduling

Champ	Description
Intervalle Schedule	Choisissez si l'intervalle de planification doit être activé. Saisissez l'intervalle en secondes après lequel le système vérifie respectivement si des événements configurés se sont produits. Les valeurs possibles sont comprises entre *0* et *65535*. Nous recommandons une valeur de *300* (précision à 5 minutes).

15.7 Surveillance

Ce menu vous permet de configurer un contrôle de joignabilité automatique pour les hôtes ou interfaces, ainsi que des tests de Ping automatiques.

Note

Cette fonction ne peut pas être configurée sur votre appareil pour les connexions authentifiées via un serveur RADIUS.

15.7.1 Hôtes

Le menu **Services locaux**->**Surveillance**->**Hôtes** affiche la liste de tous les hôtes surveillés.

15.7.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres tâches de surveillance supplémentaires.

Le menu **Services locaux**->**Surveillance**->**Hôtes**->**Nouveau** se compose des champs suivants :

Champ du menu Paramètres de l'hôte

Champ	Description
ID de groupes	Si la joingabilité d'un groupe d'hôtes ou de al passerelle par défaut doit être surveillée par votre appareil, vous devez sélectionner un identifiant pour le groupe ou la passerelle par défaut. Les identifiants de groupes sont créés automatiquement entre *0* et *255*. Si aucune entrée n'a encore été créée, l'option *Nouvelle ID* génère un nouveau groupe. Si des entrées sont disponibles, il est possible de sélectionner parmi les groupes créés. Chacun des hôtes à surveiller doit être affecté à un groupe. L'action configurée dans **Interface** n'est exécutée que si aucun membre du groupe n'est joignable.

Champs du menu Trigger

Champ	Description
Adresse IP surveillée	Saisissez l'adresse IP de l'hôte à surveiller. Valeurs possibles : • *Passerelle par défaut* (valeur par défaut) : La passerelle par défaut est surveillée. • *Spécifique*: Saisissez dans le champ de saisie ci-contre l'adresse IP de l'hôte à surveiller.
Adresse IP source	Choisissez comment déterminer l'adresse IP que votre appareil utilise comme adresse source du paquet envoyé à l'hôte à surveiller. Valeurs possibles : • *Automatique* (valeur par défaut) : L'adresse IP est déterminée automatiquement. • *Spécifique*: Saisissez l'adresse IP dans le champ de saisie ci-contre.
Intervalle	Indiquez l'intervanne (en secondes) à utiliser pour le contrôle de la joignabilité de l'hôte. Les valeurs possibles sont comprises entre *1* et *65536*.

Champ	Description
	La valeur par défaut est *10*. Au sein d'un groupe, le plus petit **Intervalle** des membres du groupe est utilisé.
Tentatives réussies	Indiquez le nombre de Pings devant obtenir une réponse afin que l'hôte soit considéré comme joignable. Ce paramétrage vous permet par exemple de définir à partir de quel moment un hôte est de nouveau considéré comme joignable et sera utilisé à la place d'un appareil de secours. Les valeurs possibles sont comprises entre *1* et *65536*. La valeur par défaut est *3*.
Tentatives échouées	Indiquez le nombre de Pings ne devant obtenir aucune réponse afin que l'hôte soit considéré comme non joignable. Ce paramétrage vous permet par exemple de définir à partir de quel moment un hôte n'est plus considéré comme joignable et qu'un appareil de secours sera utilisé à sa place. Les valeurs possibles sont comprises entre *1* et *65536*. La valeur par défaut est *3*.
Action à exécuter	Choisissez l'**Action** à exécuter. Pour la plupart des actions, il convient de sélectionner une **Interface** à laquelle se réfère l'**Action**. Toutes les interfaces physiques et virtuelles sont sélectionnables. Choisissez pour chaque interface si elle doit être activée (*Activer*), désactivée (*Désactiver*, valeur par défaut) ou réinitialisée (*Réinitialiser*), ou si la connexion doit être établie à neuf (*Composer à nouveau*). L'option **Action** = *Surveiller* vous permet de surveiller l'adresse IP indiquée sous **Adresse IP surveillée**. Ces informations peuvent être utilisées pour d'autres fonctions telle que l'**Adresse IP surveillée**.

15.7.2 Interfaces

Le menu **Services locaux**->**Surveillance**->**Interfaces** affiche la liste de toutes les interfaces surveillées.

15.7.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer la surveillance d'autres interfaces.

Le menu **Services locaux**->**Surveillance**->**Interfaces**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Interface surveillée	Sélectionnez sur votre appareil l'interface à surveiller.
Trigger	Sélectionnez l'état ou la transition d'état de l'**Interface surveillée**, qui doit déclencher une certaine **Action de l'interface**. Valeurs possibles : • *Interface activée.* (valeur par défaut) • *Interface désactivée.*
Action de l'interface	Sélectionnez l'action qui doit suivre l'état ou la transition d'état défini dans le **Trigger**. L'action est appliquée à la ou aux interfaces sélectionnées dans l'**Interface**. Valeurs possibles : • *Activer* (valeur par défaut) : Activation de ou des interfaces • *Désactiver*: Désactivation de ou des interfaces
Interface	Choisissez pour quelle(s) interface(s) l'action définie sous **Interface** doit être exécutée. Toutes les interfaces physiques et virtuelles, ainsi que les options *Toutes les interfaces PPP* et *Toutes les interfaces IPSec* sont sélectionnables.

15.7.3 Ping-Generator

Le menu **Services locaux**->**Surveillance**->**Ping-Generator** affiche la liste de tous les Pings configurés qui sont générés automatiquement.

15.7.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres Pings supplémentaires.

Le menu **Services locaux**->**Surveillance**->**Ping-Generator**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Adresse IP de destination	Saisissez l'adresse IP vers laquelle un Ping doit être envoyé automatiquement.
Adresse IP source	Saisissez l'adresse IP source des paquets de demande d'écho ICMP sortants. Valeurs possibles : • *Automatique*: L'adresse IP est déterminée automatiquement. • *Spécifique* (valeur par défaut) : Saisissez l'adresse IP dans le champ de saisie ci-contre, par ex. pour tester un routage étendu spécifique.
Intervalle	Saisissez l'intervalle en secondes pendant lequel le Ping doit être envoyé à l'adresse indiquée dans l'**Adresse IP distante**. Les valeurs possibles sont comprises entre *1* et *65536*. La valeur par défaut est *10*.
Tentatives	Saisissez le nombre de tests de Ping à réaliser jusqu'à ce que l'**Adresse IP de destination** est considérée comme *Non accessible*. La valeur par défaut est *3*.

15.8 UPnP

« Universal Plug and Play » (UPnP) permet l'utilisation des services de messagerie actuels (par ex. les conférences vidéo /audio en temps réel) comme communication pair-à-pair, dans quel cas l'un des pairs se trouve en amont une passerelle avec fonction NAT active.

UPnP permet (souvent) aux systèmes d'exploitation à base Windows de prendre le contrôle des autres appareils du réseau local avec fonctionnalité UPnP et de les pilotes. Il s'agit notamment des passerelles, points d'accès et serveurs d'imprimante. Aucun pilote d'appareil n'est nécessaire, puisque des protocoles communs et connus sont utilisés, par ex. TCP/IP, HTTP et XML.

Votre passerelle permet l'utilisation du sous-système de l'équipement de passerelle Internet (« Internet Gateway Device » – IGD) disponible dans le spectre de fonctions UPnP.

Dans un réseau en amont d'une passerelle avec fonction NAT active, les ordinateurs configurés pour UPnP réagissent comme des clients UPnP LAN. A cet effet, la fonction UPnP doit être activée sur l'ordinateur.

Le port prédéfini de la passerelle via lequel la communication UPnP entre les clients UPnP LAN et la passerelle transite, est le *5678*. Le client UPnP LAN sert alors de point de commande de service (« Service Cotnrol Point »), c'est-à-dire qu'il reconnait et commande les appareils UPnP du réseau.

Les ports affectés dynamiquement par MSN Messenger par exemple se situent dans une plage entre *5004* à *65535*. Les ports sont validés sur demande et en interne par la passerelle, c'est-à-dire au démarrage d'une transmission audio / vidéo dans Messenger. Après avoir terminé l'application, les ports sont refermés immédiatement.

La communication pair-à-pair est initiée via les serveurs SIP publics, et seules les informations des deux clients sont transmises. Ensuite, les clients communiquent directement entre eux.

Vous trouverez de plus amples informations sur l'UPnP sous *www.upnp.org*.

15.8.1 Interfaces

Dans ce menu, vous pouvez configurer les paramètres UPnP pour chaque interface individuelle de votre passerelle.

Vous pouvez définir si les demandes UPnP des clients sont acceptées via l'interface respective (pour les demandes provenant du réseau local) et/ou si l'interface peut être contrôlée via des demandes UPnP.

Le menu **Services locaux**->**UPnP**->**Interfaces** se compose des champs suivants :

Champs du menu Interfaces

Champ	Description
Interface	Permet d'afficher le nom de l'interface pour laquelle des paramétrages UPnP sont réalisés. L'entrée ne peut pas être modifiée.
Répondre à la requête du client	Définissez si les demandes UPnP des clients reçues via l'interface respectif (depuis le réseau local) font l'objet de réponses. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
L'interface est contrôlée UPnP	Définissez si la configuration NAT de cette interface est contrôlée par UPnP Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.

15.8.2 Général

Ce menu vous permet de procéder à des configurations de base UPnP.

Le menu **Services locaux**->**UPnP**->**Général** se compose des champs suivants :

Champs du menu Général

Champ	Description
État UPnP	Décidez comment la passerelle traite les demandes UPnP du LAN. Sélectionnez *Activé* pour activer la fonction. La passerelle procède aux validations conformément aux paramètres contenus dans la demande du client UPnP LAN, indépendamment de l'adresse IP du client UPnP LAN. La fonction est désactivée par défaut. La passerelle rejette les demandes UPnP, aucune validation NAT n'est réalisée.

Champ	Description
Port UPnP TCP	Saisissez le numéro du port sur lequel la passerelle écoute les demandes UPnP. Les valeurs possibles sont comprises entre *1* et *65535*, la valeur par défaut est *5678*.

15.9 Passerelle hotspot

La **Hotspot Solution** sert à la mise à disposition d'accès Internet publics (par WLAN ou Ethernet câblé). La solution est adaptée à la constitution de solutions Hotspot de petite et moyenne envergure pour des cafés, des hôtels, des entreprises, des logements collectifs, des campings, etc.

La **Hotspot Solution** se compose d'une passerelle **Gigaset** installée sur place (avec point d'accès WLAN propre, appareil WLAN supplémentaire connecté ou LAN câblé) et du serveur de Hotspot, qui est installé en position centrale dans un centre de calcul. Un terminal d'administration (par ex. le PC de la réception de l'hôtel) sert à gérer le compte d'exploitant sur le serveur, par ex. la saisie d'inscriptions, la création de tickets, les analyses statistiques, et.

Déroulement de la procédure de connexion au serveur de Hotspot

- Si un nouvel utilisateur se connecte au Hotspot, une adresse IP lui est affectée automatiquement par DHCP.
- Dès qu'il tente d'ouvrir un site Internet quelconque dans son navigateur, l'utilisateur est redirigé vers la page d'accueil / de login.
- Après avoir saisi ses données de connexion (nom d'utilisateur/mot de passe), celles-ci sont envoyées en tant que connexion RADIUS au serveur RADIUS (serveur Hotspot) central.
- Après le succès de la connexion, la passerelle valide l'accès à Internet.
- A intervalles réguliers, la passerelle transmet pour chaque utilisateur des informations complémentaires au serveur RADIUS pour enregistrer des données de comptabilité.
- Au terme de la validité du ticket, l'utilisateur est déconnecté automatiquement et redirigé vers la page d'accueil / de login.

Conditions préalables

Afin de pouvoir exploiter un Hotspot, le client à besoin :

- d'un appareil **Gigaset** comme passerelle Hotspot avec un accès Internet actif et des entrées de serveur Hotspot configurées pour la connexion et la comptabilité (voir menu **Gestion du système**->**Authentification distante**->**RADIUS**->**Nouveau** avec **Description du groupe** `Groupe par défaut 0`).
- **Gigaset** Hébergement de Hotspot (Réf. article 5510000198 ou 5510000197)
- Données d'accès
- Documentation
- Licence du logiciel

  Veuillez noter que vous devez d'abord activer la licence.

  - Ouvrez *www.bintec-elmeg.com* puis **Service/Assistance** -> **Services** -> **Services en ligne**.

  - Saisissez les données nécessaires (reporter-vous à cet effet aux explications figurant sur la fiche de licence) et suivez les instructions de l'activation de licence en ligne.

  - Vous recevrez alors les données de connexion du serveur Hotspot.

Note

L'activation peut prendre 2 à 3 jours ouvrés.

Données d'accès pour la configuration de la passerelle

IP du serveur RADIUS	62.245.165.180
Mot de passe du serveur RADIUS	Défini par Gigaset GmbH
Domaine	Est défini par le client/commerçant spécialisé selon les besoins du client.
Réseau « Walled Garden »	Est défini par le client/commerçant spécialisé selon les besoins du client.
URL du serveur Walled Garden	Est défini par le client/commerçant spécialisé selon les besoins du client.
URL des Conditions Générales de Vente	Est défini par le client/commerçant spécialisé selon les besoins du client.

Données d'accès pour la configuration du serveur Hotspot

URL d'administration	https://hotspot.bintec-elmeg.com/
Nom d'utilisateur	Est défini au cas par cas par bintec elmeg.

Mot de passe	Est défini au cas par cas par bintec elmeg.

Note

Reportez-vous également à l'atelier WLAN Hotspot, que vous pourrez télécharger depuis *www.bintec-elmeg.com* .

15.9.1 Passerelle hotspot

Le menu **Passerelle hotspot** vous permet de configurer la passerelle **Gigaset** installée sur site pour la **Hotspot Solution**.

Le menu **Services locaux**->**Passerelle hotspot**->**Passerelle hotspot** affiche la liste de tous les réseaux Hotspot configurés.

L'option **Activé** permet d'activer ou de désactiver l'entrée correspondante.

15.9.1.1 Editer ou Nouveau

Le menu **Services locaux**->**Passerelle hotspot**->**Passerelle hotspot**-> vous sert à configurer les réseaux Hotspot. Actionnez le bouton **Nouveau** pour configurer d'autres réseaux Hotspot.

Le menu **Services locaux**->**Passerelle hotspot**->**Passerelle hotspot**-> se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Interface	Sélectionnez l'interface à laquelle le Hotspot LAN ou WLAN est connecté. Lors du fonctionnement par LAN, vous devez saisir ici l'interface Ethernet (par ex. en1-0). Lors du fonctionnemnet par WLAN, vous devez sélectionner l'interface WLAN à laquelle le point d'accès est connecté.

Champ	Description
	Attention Pour des raisons de sécurité, la configuration de votre appareil n'est pas possible via l'interface configurée pour le Hotspot. Il convient donc de choisir avec soin l'interface que vous souhaitez utiliser pour le Hotspot ! Si vous sélectionnez ici l'interface via laquelle à lieu la session de configuration actuelle, la connexion actuelle est perdue. Vous devrez alors vous reconnecter via une interface joignable, non configurée pour le Hotspot, pour poursuivre la configuration de votre appareil.
Domaine sur le serveur hotspot	Saisissez le nom de domaine utilisé lors de la configuration du serveur Hotspot pour ce client. Le nom de domaine est nécessaire afin que le serveur Hotspot puisse différencier les divers mandants (clients).
Walled Garden	Activez cette fonction si vous souhaitez définir un espace de pages Internet limité et gratuit (Intranet). La fonction est désactivée par défaut.
Walled Network / **Masque réseau**	Uniquement si **Walled Garden** est activé. Saisissez l'adresse réseau du **Walled Network** et le **Masque réseau** correspondant du serveur Intranet. Pour l'espace d'adresse résultant pour le **Walled Network** / **Masque réseau**, les clients ne requièrent pas d'authentification. Exemple : Si vous saisissez 192.168.0.0 / 255.255.255.0, toutes les adresses IP de 192.168.0.0 à 19.168.0.255 sont libres. Si vous saisissez 192.168.0.1 / 255.255.255.255, seule l'adresse IP 192.168.0.1 est libre.
URL Walled Garden	Uniquement si **Walled Garden** est activé. Saisissez l'**URL Walled Garden** du serveur Intranet. Les sites Internet librement accessibles doivent être joignables via cette

Champ	Description
	adresse.
Conditions de vente	Uniquement si **Walled Garden** est activé. Saisissez dans le champ de saisie **Conditions de vente** l'adresse des CGV sur le serveur Intranet ou sur un serveur public, par ex. fttp://www.webserver.fr/cgv.htm. La page doit se situer dans l'espace d'adresses du réseau Walled Garden.
Noms de domaines supplémentaires à accès libre	Uniquement si **Walled Garden** est activé. A l'aide du bouton **Ajouter**, ajoutez des URL ou adresses IP supplémentaires. Les sites Internet sont joignables via ces adresses supplémentaires librement accessibles.
Langue pour fenêtre de connexion	Ici, vous pouvez choisir la langue pour la page d'accueil / de login. Les langues suivantes sont supportées : *English*, *Deutsch*, *Italiano*, *Français*, *Español*, *Português* et *Nederlands*. La langue peut être commutée à tout moment sur la page d'accueil / de login.

Le menu **Paramètres étendus** se compose des champs suivants :

Champs du menu Paramètres étendus

Champ	Description
Type de ticket	Sélectionnez le type de ticket. Valeurs possibles : • *Voucher*: Seul le nom d'utilisateur devra être saisi. Définissez un mot de passe standard dans le champ de saisie. • *Nom de l'utilisateur/Mot de passe* (valeur par défaut) : Le nom d'utilisateur et le mot de passe devront être saisis.
Client hotspot admis.	Ici, vous pouvez définir quels types d'utilisateurs sont autorisés à se connecter au Hotspot. Valeurs possibles :

Champ	Description
	• *Tous*: Tous les clients sont autorisés. • *Client DHCP*: Empêche la connexion d'utilisateurs qui n'ont pas obtenu d'adresse IP par DHCP.
Fenêtre de connexion	Activez ou désactivez la fenêtre de connexion. La fenêtre de connexion de la page d'accueil HTML se compose de deux blocs de transmission de données. Lorsque la fonction est activée, le formulaire d'enregistrement s'affiche sur le côté gauche. Lorsque la fonction est désactivée, seule la page Internet avec des informations, des publicités et/ou des liens vers les sites Internet librement accessibles s'affiche. La fonction est activée par défaut.
Fenêtre pop-up pour affichage de l'état	Définissez si l'appareil utilise des fenêtres en superposition pour l'affichage de l'état. La fonction est activée par défaut.
Timeout par défaut en cas d'inactivité	Activez ou désactivez le **Timeout par défaut en cas d'inactivité**. Si un utilisateur ne génère pas de trafic de données pendant un temps imparti paramétrable, il est déconnecté du Hotspot. La fonction est activée par défaut. La valeur par défaut est *600* secondes.

15.9.2 Options

Le menu **Services locaux**->**Passerelle hotspot**->**Options** sert à procéder à des paramétrages généraux pour le Hotspot.

Le menu **Services locaux**->**Passerelle hotspot**->**Options** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Hôte pour plusieurs	Si pour un client, plusieurs sites (filiales) ont été configurées

Champ	Description
sites	sur le serveur Hotpsot, vous devez saisir ici la valeur de l'identifiant NAS (paramètre de serveur RADUIS) qui a été enregistré sur le serveur Hotspot pour ce site.

15.10 Wake-On-LAN

La fonction **Wake-On-LAN (WOL)** permet de démarrer les appareils de réseau désactivés à l'aide d'un carte réseau intégrée. La carte réseau doit être alimentée électriquement en continu, même lorsque l'ordinateur est éteint. Vous pouvez définir à l'aide de filtres et de chaînes de règles les conditions devant être remplies pour l'envoi du paquet dit Magic, ainsi que sélectionner les interfaces qui doivent être surveillées quant aux chaînes de règles définies. La configuration des filtres et chaînes de règles correspond pour l'essentiel à la configuration des filtres et chaînes de règles dans le menu **Règles d'accès**.

15.10.1 Filtre Wake-On-LAN

Le menu **Wake-On-LAN**->**Filtre Wake-On-LAN** affiche la liste de tous les filtres WOL configurés.

15.10.1.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres filtres supplémentaires.

Le menu **Wake-On-LAN**->**Filtre Wake-On-LAN**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Description	Saisissez la désignation du filtre.
Service	Sélectionnez l'un des services préconfigurés. D'origine, une liste complète de services est préconfigurée, dont : • *activity* • *apple-qt* • *auth* • *chargen*

Champ	Description
	• *clients_1* • *daytime* • *dhcp* • *discard* La valeur par défaut est *Quelconque*.
Journal	Sélectionnez un protocole. L'option *Quelconque* (valeur par défaut) convient à tous les protocoles.
Type	Uniquement pour **Journal** = *ICMP* Sélectionnez un type. Valeurs possibles : *Quelconque*, *Echo reply*, *Destination unreachable*, *Source quench*, *Rediriger*, *Echo*, *Time exceeded*, *Timestamp*, *Timestamp reply*. Voir la RFC 792. La valeur par défaut est *Quelconque*.
Etat de la connexion	Si **Journal** = *TCP*, vous pouvez définir un filtre qui tient compte de l'état des connexions TCP. Valeurs possibles : • *Etabli* : le filtre tient compte des paquets TCP qui n'ouvrent pas de nouvelle connexion TCP en cas de routage via la passerelle. • *Quelconque* (valeur par défaut) : Le filtre tient compte de tous les paquets TCP.
Adresse IP de destination/Masque de réseau	Saisissez les adresses IP de destination des paquets de données, ainsi que les masques de réseau correspondants.
Port de destination/ zone	Uniquement pour **Journal** = *TCP* ou *UDP* Saisissez un numéro de port de destination ou une plage de numéros de ports de destination. Valeurs possibles :

Champ	Description
	• *-Tous-* (valeur par défaut) : Le port de destination n'est pas spécifié de manière plus détaillée. • *Saisir le port* : saisissez un port de destination. • *Saisir la plage de ports* : saisissez une plage de ports de destination.
Adresse IP source/ Masque de réseau	Saisissez les adresses IP source des paquets de données, ainsi que les masques de réseau correspondants.
Port source/zone	Uniquement pour **Journal** = *TCP* ou *UDP* Saisissez un numéro de port source ou une plage de numéros de ports source. Valeurs possibles : • *-Tous-* (valeur par défaut) : Le port de destination n'est pas spécifié de manière plus détaillée. • *Saisir le port* : saisissez un port de destination. • *Saisir la plage de ports* : saisissez une plage de ports de destination.
Filtre DSCP/TOS (couche 3)	Sélectionnez le type de service (TOS, Type of Service). Valeurs possibles : • *Ignorer* (valeur par défaut) : Le type de service n'est pas pris en compte. • *Valeur binaire DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format binaire, 6 bits). • *Valeur décimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format décimal). • *Valeur hexadécimale DSCP* : le champ Differentiated Services Code Point selon la RFC 3260 est utilisé pour signaler la priorité des paquets IP (données au format hexadécimal). • *Valeur binaire TOS* : la valeur TOS est indiquée au format binaire, p. ex. 00111111. • *Valeur décimale TOS* : la valeur TOS est indiquée au format décimal, p. ex. 63.

Champ	Description
	• *Valeur hexadécimale TOS* : la valeur TOS est indiquée au format hexadécimal, p. ex. 3F.
Filtre COS (802.1p/Layer 2)	Introduisez la classe de service des paquets IP (Class of Service, CoS). Les valeurs possibles sont des nombres entiers compris entre *0* et *7*. Plage de valeurs de *0* à *7*. La valeur par défaut est *Ignorer*.

15.10.2 Règles WOL

Le menu **Wake-On-LAN**+**Règles WOL** affiche la liste de toutes les règles WOL configurées.

15.10.2.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres règles supplémentaires.

Le menu **Wake-On-LAN**+**Règles WOL**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Chaîne de règles Wake-On-LAN	Indiquez si vous souhaitez créer une chaîne de règle ou en éditer une existante. Valeurs possibles : • *Nouveau* (valeur par défaut) : Ce paramètre vous permet de créer une chaîne de règle. • *<Nom de la chaîne de règles>* : Permet d'afficher une chaîne de règles déjà créée, que vous pouvez sélectionner et éditer.
Description	Uniquement pour la **chaîne de règles Wake-On-LAN** = *Nouveau* Saisissez la désignation de la chaîne de règle.

Champ	Description
Filtre Wake-On-LAN	Sélectionnez un filtre WOL. Pour une nouvelle chaîne de règle, sélectionnez le filtre qui doit être défini au premier plan de la chaîne de règle. Pour une chaîne de règle existante, sélectionnez le filtre qui doit être associé à la chaîne de règle. Pour pouvoir sélectionner un filtre, au moins un filtre doit être configuré dans le menu **Wake-On-LAN**+**Règles WOL**.
Action	Déterminez la procédure à suivre avec un paquet de données filtré. Valeurs possibles : • *Appeler WOL si le filtre est correct*: Exécuter WOL lorsque le filtre correspond. • *Appeler WOL si le filtre n'est pas correct*: Exécuter WOL lorsque le filtre ne correspond pas. • *Refuser WOL si le filtre est correct*: Ne pas exécuter WOL lorsque le filtre correspond. • *Refuser WOL si le filtre n'est pas correct*: Ne pas exécuter WOL lorsque le filtre ne correspond pas. • *Ignorer la règle et passer à la règle suivante*: Cette règle est ignorée et la règle suivante de la chaîne est contrôlée.
Type	Choisissez si le paquet Wake on LAN Magic doit être envoyé comme paquet UDP ou comme bloc de transmission de données Ethernet via l'interface définie dans **Envoyer paquet WOL via l'interface**.
Envoyer paquet WOL via l'interface	Sélectionnez l'interface via laquelle le paquet Wake on LAN Magic doit être envoyé.
Adresse MAC cible	Uniquement pour **Action** = *Appeler WOL si le filtre est correct* et *Appeler WOL si le filtre n'est pas correct* Saisissez l'adresse MAC de l'appareil de réseau qui doit être activé par WOL.
Mot de passe	Uniquement pour **Action** = *Appeler WOL si le filtre*

Champ	Description
	est correct et *Appeler WOL si le filtre n'est pas correct* Si l'appareil de réseau à activer supporte la fonction « SecureOn », vous devez saisir ici le mot de passe de cet appareil. L'appareil n'est activé que si l'adresse MAC et le mot de passe sont corrects.

15.10.3 Affectation des interfaces

Dans ce menu, les chaînes de règles configurées sont affectées à des interfaces individuels qui seront surveillés quant à ces chaînes de règles.

Le menu **Wake-On-LAN**+**Affectation des interfaces** affiche la liste de toutes les affectations d'interfaces configurées.

15.10.3.1 Editer ou Nouveau

Sélectionnez le symbole pour traiter les entrées existantes. Actionnez le bouton **Nouveau** pour configurer d'autres entrées supplémentaires.

Le menu **Wake-On-LAN**+**Affectation des interfaces**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Interface	Sélectionnez l'interface à laquelle attribuer une chaîne de règle configurée.
Chaîne de règle	Sélectionnez une chaîne de règle.

Chapitre 16 Maintenance

Ce menu offre de nombreuses fonctions pour la maintenance de votre appareil. Vous y trouverez notamment un menu pour tester l'accessibilité au sein du réseau. Vous pouvez y gérer vos fichiers de configuration système. Si un logiciel système plus récent est disponible, l'installation peut être réalisée à l'aide de ce menu. Si vous avez besoin de langues supplémentaires pour l'interface de configuration, vous pouvez les importer. Ce menu permet également de déclencher le redémarrage du système.

16.1 Diagnostic

Dans le menu **Maintenance**->**Diagnostic** vous pouvez tester l'accessibilité d'hôtes individuels, la résolution de noms de domaine et certaines routages.

16.1.1 Test Ping

Le test de Ping vous permet de vérifier si un hôte spécifique du LAN ou une adresse Internet sont joignables. Le champ **Sortie** affiche les messages du test de Ping. La saisie de l'adresse IP à tester dans le champ **Envoyer une commande Ping vers l'adresse à fin de test**, suivi de l'actionnement du bouton **Démarrer**, lance le test de Ping.

16.1.2 Test DNS

Le test de DNS vous permet de vérifier si la résolution du nom de domaine d'un hôte spécifique est correcte. Le champ **Sortie** affiche les messages du test de DNS. La saisie du nom de domaine à tester dans le champ **Adresse DNS**, suivi de l'actionnement du bouton **Démarrer**, lance le test de DNS.

16.1.3 Test Traceroute

Le test Traceroute vous permet d'afficher le routage vers une adresse spécifique (adresse IP ou nom de domaine), dans la mesure où elle est joignable. Le champ **Sortie** affiche les messages du test Traceroute. La saisie de l'adresse à tester dans le champ **Adresse Traceroute**, suivi de l'actionnement du bouton **Démarrer**, lance le test Traceroute.

16.2 Logiciel et configuration

Ce menu vous permet de gérer la version logicielle de votre appareil, vos fichiers de configuration ainsi que les langues de la **GUIs**.

16.2.1 Options

Votre appareil est équipé de la version la plus récente du logiciel système disponible à sa date de fabrication. Le cas échéant, des versions plus récentes sont actuellement disponibles. Vous devrez donc éventuellement effectuer une mise à jour du logiciel.

Chaque nouveau logiciel système comprend de nouvelles fonctions, offre plus de puissance et corrige les éventuels dysfonctionnements de la version antérieure. Vous trouverez le logiciel système actuel sous *www.gigasetpro.com* . Vous y trouverez aussi les documentations actuelles.

Important

Si vous effectuez une mise à jour du logiciel, vous devez impérativement respecter le consignes figurant dans les « Release Notes » correspondantes. Elles décrivent toutes les modifications introduites avec le nouveau logiciel système.

Si le processus de mise à jour est interrompu (par ex. suite à une panne de secteur pendant la mise à jour), votre appareil peut ne plus démarrer. N'éteignez pas votre appareil pendant la mise à jour.

Dans certains rares cas, nous recommandons également une mise à jour de BOOTmonitor et/ou Logic. Dans ce cas, cette recommandation figure explicitement dans les instructions de mise à jour, les « Release Notes ». N'effectuez de mise à jour de BOOTmonitor ou Logic que si Gigaset GmbH le recommande explicitement.

Flash

Votre appareil enregistre sa configuration dans des fichiers de configuration dans l'EEPROM Flash (electrically erasable programmable read-only memory). Même lorsque votre appareil est éteint, les données sont conservées dans la mémoire Flash.

RAM

La mémoire vive (RAM) contient la configuration actuelle et toutes les modifications que vous apportez à votre appareil pendant son fonctionnement. Le contenu de la mémoire RAM est perdu lorsque vous éteignez votre appareil. Si vous modifiez la configuration et souhaitez conserver ces modifications après le prochain démarrage de votre appareil, vous devez enregistrer la configuration modifiée dans la mémoire Flash. Bouton **Enregistrer la configuration** au-dessus de la zone de navigation de la **GUIs**. La configuration est alors enregistré dans un fichier appelé *boot* dans la mémoire Flash. Lors du démarrage de votre appareil, le fichier de configuration *boot* est utilisé par défaut.

Actions

Les données dans la mémoire flash peuvent être copiées, déplacées, supprimées et créées. Il est également possible de transférer des fichiers de configuration par HTTP entre votre appareil et un hôte.

Format des fichiers de configuration

Le format de fichier du fichier de configuration permet le cryptage et assure la compatibilité lors de la restauration de la configuration sur la passerelle vers différentes versions du logiciel système. Il s'agit d'un format CSV, qui peut être lu et modifié sans problèmes. Vous pouvez en outre afficher les données correspondantes sous la forme d'un aperçu, p. ex. à l'aide de Microsoft Excel. Les fichiers de sauvegarde de la configuration peuvent être mémorisés avec un cryptage par l'administrateur. Lors de l'envoi de la configuration par e-mail (par ex. à des fins d'assistance), les données de configuration confidentielles peuvent être entièrement protégées le cas échéant. Ainsi, les actions « Exporter la configuration », « Exporter la configuration avec informations d'état » et « Charger la configuration » vous permettent de sauvegarder et de charger des fichiers. Si vous souhaitez sauvegarder un fichier de configuration à l'aide des actions « Exporter la configuration » et « Exporter la configuration avec informations d'état », vous pouvez définir si le fichier de configuration doit être enregistré crypté ou non crypté.

Attention

Si vous avez sauvegardé un fichier de configuration dans un ancien format avec l'instruction `put` de l'enveloppe SNMP, le chargement dans l'appareil ne peut pas être garanti. De ce fait, nous recommandons de ne plus utiliser l'ancient format.

Le menu **Maintenance**->**Logiciel et configuration**->**Options** se compose des champs suivants :

Champs du menu Logiciel actuellement installé

Champ	Description
BOSS	Affiche la version actuelle du logiciel, qui est chargée sur votre appareil.
Logique du système	Affiche la logique système actuelle, qui est chargée sur votre appareil.

Champs du menu Options du logiciel et de la configuration

Champ	Description
Action	Sélectionnez l'action que vous souhaitez exécuter. Une fois les tâches respectives exécutées, une fenêtre s'affiche, vous indiquant les étapes suivantes. Valeurs possibles : • *Pas d'action* (valeur par défaut) : • *Exporter la configuration*: Le fichier de configuration **Nom de fichier actuel sur le flash** est transmis à votre hôte local. Si vous actionnez le bouton **Démarrer**, un dialogue s'affiche dans lequel vous pouvez choisir le répertoire d'enregistrement sur votre PC et saisir le nom de fichier souhaité. • *Importer la configuration*: Choisissez dans **Nom du fichier** un fichier de configuration pour l'importation. Remarque : Cliquez sur **Démarrer** pour charger le fichier dans la mémoire Flash de l'appareil, dans un premier temps sous le nom *boot*. Pour l'activer, vous devez redémarrer l'appareil. Remarque : Le fichier à importer doit être au format CSV ! • *Copier la configuration*: Le fichier de configuration dans le champ **Nom du fichier source** est enregistré sous **Nom du fichier de destination**. • *Supprimer la configuration*: La configuration dans le champ **Sélectionner le fichier** est effacée. • *Renommer la configuration*: Le fichier de configuration dans le champ **Sélectionner le fichier** est renommé en **Nouveau nom du fichier**. • *Restaurer la sauvegarde* : Uniquement si sous **Enregistrer la configuration** avec le paramétrage *Enregistrer la configuration et sauvegarder la*

Champ	Description
	configuration de démarrage précédente la configuration actuelle a été enregistrée comme configuration de démarrage et que de plus, la configuration de démarrage précédente a été archivée. Vous pouvez recharger la configuration de démarrage archivée. • *Supprimer logiciel/firmware*: Le fichier dans le champ **Sélectionner le fichier** est supprimé. • *Importer la langue*: Vous pouvez charger des langues supplémentaires pour la **GUI** sur votre appareil. Vous pouvez télécharger les fichiers sur votre PC depuis l'espace de téléchargement de *www.gigasetpro.com* , puis les charger dans votre appareil. • *Mettre à jour le logiciel système*: Vous pouvez lancer une mise à jour du logiciel système, de la logique ADSL et du BOOTmonitor. • *Importer les fichiers Voice Mail Wave* (Ne s'affiche que si une carte SD est enfichée) : Choisissez dans **Nom de fichier** le fichier *vms_wavfiles.zip* pour l'importation. • *Exporter la configuration avec les informations d'état*: La configuration active de la mémoire RAM est transmise à votre hôte local. Si vous cliquez sur le bouton **Démarrer**, un dialogue s'affiche dans lequel vous pouvez choisir le répertoire d'enregistrement sur votre PC et saisir le nom de fichier souhaité.
Nom de fichier actuel sur le flash	Pour **Action** = *Exporter la configuration* Sélectionnez le fichier de configuration à exporter.
Inclure les certificats et les clés	Pour **Action** = *Exporter la configuration* Choisissez si l'**Action** sélectionnée doit s'appliquer aussi aux certificats et codes. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Cryptage de la configuration	Uniquement pour **Action** = *Exporter la configuration*, *Importer la configuration*, *Exporter la configuration avec les informations d'état*

Champ	Description
	Indiquez si les données de l'**Action** sélectionnée doivent être cryptées. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut. Si la fonction est activée, vous pouvez saisir le **Mot de passe** dans le champ de texte.
Nom du fichier	Uniquement pour **Action** = *Importer la configuration*, *Importer la langue*, *Mettre à jour le logiciel système* Saisissez le chemin d'accès du fichier et le nom du fichier ou sélectionnez le fichier avec **Parcourir...** à l'aide du gestionnaire de fichiers.
Nom du fichier source	Uniquement pour **Action** = *Copier la configuration* Sélectionnez le fichier source à copier.
Nom du fichier de destination	Uniquement pour **Action** = *Copier la configuration* Saisissez le nom de la copie.
Sélectionner le fichier	Uniquement pour **Action** = *Supprimer la configuration*, *Renommer la configuration* ou *Supprimer logiciel/firmware* Choisissez le fichier ou la configuration qui doit être renommé ou supprimé.
Nouveau nom du fichier	Uniquement pour **Action** = *Renommer la configuration* Saisissez le nouveau nom du fichier de configuration.
Source	Uniquement pour **Action** = *Mettre à jour le logiciel système* Sélectionnez la source pour la mise à jour. Valeurs possibles : • *Fichier local* (valeur par défaut) : Le fichier de logiciel

Champ	Description
	système est enregistré localement sur votre PC. • *Serveur HTTP*: Le fichier est enregistré sur le serveur distant indiqué dans l'**URL**. • *Logiciel en cours du serveur de mise à jour*: le fichier se trouve sur le serveur de mise à jour officiel.
URL	Uniquement pour **Action** = *Mettre à jour le logiciel système* et **Source** = *Serveur HTTP* Saisissez l'URL du serveur de mise à jour depuis lequel vous souhaitez charger le fichier de logiciel système.

16.3 Mise à jour de téléphone

Dans le menu **Mise à jour de téléphone** vous pouvez actualiser le logiciel de vos téléphones système.

Note

Avant de lancer la mise à jour du logiciel de vos téléphones système, vous devez charger le logiciel dans le menu **Maintenance**->**Mise à jour de téléphone**->**Fichiers du logiciel système** sur votre carte SD.

16.3.1 Gigaset Téléphone

Le menu **Gigaset Téléphone** contient la liste des téléphones Gigaset ou postes de base Gigaset connectés. Ce masque affiche les téléphones Gigaset ainsi que les postes de base DECT Gigaset, dans la mesure où le système en contient. Vous pouvez sélectionner des appareils pour la mise à jour immédiate du logiciel, ou leur permettre de télécharger systématiquement les nouveaux logiciels depuis l'installation.

Dans le cas d'une mise à jour instantanée, aucun contrôle de la version n'est effectué.

Note

Veuillez noter qu'une mise à jour immédiate du logiciel pour les systèmes DECT Multicell n'est disponible que via le configurateur réseau du système et ne peut pas être lancé depuis l'interface utilisateur du **elmeg hybird**.

Valeurs de la liste Gigaset Téléphone

Champ	Description
Description	Permet d'afficher la description saisie pour le téléphone système.
Type de téléphone	Permet d'afficher le type de téléphone système.
Adresse MAC	Permet d'afficher l'adresse MAC du téléphone système.
Version Téléphone	Permet d'afficher la version logicielle du téléphone.
Version de la carte SD	Permet d'afficher la version de la carte SD insérée.
État/État de mise à jour	Permet d'afficher l'état du téléphone système ou une barre de progression au cours d'une mise à jour. L'icône indique un téléphone système connecté, dont le logiciel système est pris en charge par votre **hybird**. L'icône indique un téléphone système non connecté, ou dont le logiciel système n'est pas pris en charge par votre **hybird**. Pour les téléphones IP, il n'existe aucune restriction quant à la mise à jour simultanée du logiciel système. Si le logiciel système d'un téléphone système n'est pas pris en charge par votre **hybird**, vous pouvez malgré tout le mettre à jour. Pendant la mise à jour d'un logiciel système, une barre de progression s'affiche.
Mise à jour autorisée	Permet d'afficher si les télépohones connectés peuvent télécharger de manière autonome les nouveaux logiciels depuis l'installation. Vous pouvez sélectionner des entrées individuelles en cochant les cases correspondantes des différentes lignes, ou les sélectionner toutes à l'aide du bouton **Sélectionner tout** ou **Désactiver tout**.
Mettre à jour immédia-	Permet d'indiquer si le logiciel du téléphone système doit être

Champ	Description
tement	mis à jour immédiatement. La fonction est activée sur un seul appareil en cochant la case correspondante. La fonction est désactivée par défaut. Vous pouvez utiliser les boutons **Sélectionner tout** ou **Désactiver tout** pour tous les appareils affichés.

16.3.2 Fichiers du logiciel système

Le menu **Maintenance**->**Mise à jour de téléphone**->**Fichiers du logiciel système** affiche les fichiers de logiciel système qui sont actuellement disponibles sur votre carte SD. Vous pouvez charger d'autres fichiers sur la carte SD.

Note

Pour les systèmes DECT, un fichier ZIP est mis à disposition, qui contient les fichiers de logiciel système, mais aussi des fichiers de langues pour **Gigaset N510 IP PRO**.

Note

Pour chaque type de téléphones, une version du fichier de logiciel peut être enregistrée sur la carte SD.

Valeurs de la liste Fichiers du logiciel système

Champ	Description
Charger le logiciel système	Enregistrez les fichiers de logiciel système sur votre carte SD.
N°	Permet d'afficher le numéro d'ordre du fichier de logiciel système sur votre carte SD.
Type de téléphone	Permet d'afficher le type de téléphone système.
Version	Permet d'afficher la version du logiciel système.

Champ	Description
État	Indique qu'un fichier de logiciel système est enregistré sur la carte SD dans le répertoire approprié.

16.3.3 Paramètres

Le menu **Maintenance**->**Mise à jour de téléphone**->**Paramètres** permet de définir une plage temporelle pour la mise à jour du logiciel système en fonction d'une période. vous pouvez enregistrer un numéro de téléphone à utiliser si la mise à jour du logiciel système a échoué. Ce numéro de téléphone peut être choisi avec le téléphone pour mettre à jour le logiciel système, lorsque le téléphone système est en mode de démarrage après une mise à jour échouée.

Le menu **Maintenance**->**Mise à jour de téléphone**->**Paramètres** se compose des champs suivants :

Champs du menu Réglage de l'heure pour la mise à jour du logiciel système du téléphone système

Champ	Description
Numéro d'appel interne	Uniquement pour les téléphones RNIS. Saisissez le numéro d'appel du serveur de mise à jour de **hybird**, que vous souhaitez appeler depuis le téléphone en cas d'échec de la mise à jour du logiciel système. Dans ce cas, vous pouvez effectuer la mise à jour depuis le téléphone. Ce numéro d'appel est automatiquement transmis au téléphone système dès que le téléphone se connecte à **hybird**. Après la transmission le numéro du téléphone s'affiche sous **Menu**->**Service**->**Mise à jour de logiciel**. L'actionnement de la touche **OK** enregistre le numéro pour la répétition du dernier appel.
Mettre à jour le logiciel système	Définissez une plage temporelle pour la mise à jour du logiciel système. Définissez à cet effet l'**Heure de début** et l'**Temps d'arrêt**.

16.4 Redémarrage

16.4.1 Redémarrage système

Ce menu vous permet de déclencher le redémarrage immédiat de votre appareil. Après le redémarrage du système, vous devez ouvrir l'**GUI** et vous connecter.

Observez à cet effet les DELS de votre appareil. La signification des DEL figure dans le manuel, chapitre **Caractéristiques techniques**.

Note

Avant tout redémarrage, assurez-vous de bien confirmer les modifications que vous avez apporté à la configuration en cliquant sur le bouton **Enregistrer la configuration**, afin qu'elles ne soient pas perdues au démarrage.

Si vous souhaitez redémarrer votre appareil, cliquez sur le bouton **OK**. Le redémarrage est exécuté.

Chapitre 17 Création de rapports externe

Ce menu vous permet de définir les messages de protocoles système enregistrés sur un ordinateur spécifique, et si l'administrateur système doit recevoir un e-mail lors de certains événements. Les informations relatives au trafic de données IP peuvent également être enregistrées en fonction des différentes interfaces. De plus, en cas de défaillance, des traps SNMP peuvent être envoyés à certains hôtes.

17.1 Journal système

Les événements dans les différents sous-systèmes de votre appareil (par ex. PPP) sont consignés sous forme de messages de protocole système (syslog). En fonction du niveau défini (huit niveaux de *Urgence* via *Informations* à *Debug*), le nombre de messages affiché est plus ou moins important.

Outre les données consignées en interne sur votre appareil, toutes les informations peuvent et doivent être transmises pour enregistrement et traitement à un ou plusieurs ordinateurs externes supplémentaires, par ex. à l'ordinateur de l'administrateur système. Les messages de protocole système enregistrés en interne sur votre appareil sont perdus lors du redémarrage.

AVERTISSEMENT

Veillez à ne transmettre les messages de protocole système qu'à un ordinateur sécurisé. Contrôlez les données régulièrement en veillant à ce qu'il reste toujours assez d'espace mémoire libre sur le disque dur de l'ordinateur.

Démon Syslog

L'enregistrement des messages de protocole système est supporté par tous les systèmes d'exploitation Unix. Sur les ordinateurs Windows, les **DIME Tools** comprennent un démon syslog qui enregistre les données et peut les répartir sur différents fichiers en fonction du contenu (disponibles dans l'espace de téléchargement sous *www.bintec-elmeg.com*).

17.1.1 Serveur Syslog

Configurez votre appareil comme serveur syslog de sorte que les messages système définis puissent être envoyés à des hôtes appropriés dans le LAN.

Ce menu vous permet de définir les messages, les conditions et les hôtes pour l'envoi.

Le menu **Création de rapports externe**->**Journal système**->**Serveur Syslog** contient la liste de tous les serveurs de protocoles système configurés.

17.1.1.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres serveurs de protocoles système.

Le menu **Création de rapports externe**->**Journal système**->**Serveur Syslog**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Adresse IP	Saisissez l'adresse IP de l'hôte auquel les messages de protocole système doivent être transmis.
Niveau	Définissez la priorité des messages de protocole système à envoyer à l'hôte. Valeurs possibles : • *Urgence* (priorité la plus haute) • *Alarme* • *Critique* • *Erreur* • *Avertissement !* • *Notification* • *Informations* (valeur par défaut) • *Debug* (priorité minimale) Seuls les messages de protocole système de priorité identique ou supérieure à celle indiquée sont transmis à l'hôte, c'est-à-dire que pour le niveau syslog *Debug*, tous les messages générés sont transmis à l'hôte.
Facility	Indiquez le dispositif syslog sur l'hôte. Ceci n'est nécessaire que si l'**hôte de log** est un ordinateur Unix. Valeurs possibles : *local0 - 7* (valeur par défaut)

Champ	Description
	local0.
Horodatage	Choisissez le format du chronotimbre du protocole système. Valeurs possibles : • *aucun* (valeur par défaut) : Aucune indication de l'heure du système • *Heure*: Heure système sans la date • *Date et heure*: Heure système avec la date
Journal	Choisissez le protocole pour le transfert des messages de protocole système. Notez que le serveur syslog doit être compatible avec le protocole. Valeurs possibles : • *UDP* (valeur par défaut) • *TCP*
Type de message	Sélectionnez le type de messages. Valeurs possibles : • *System &Accounting* (valeur par défaut) • *Système* • *Accounting*

17.2 IP-Accounting

Dans les réseaux modernes, des informations sur le type et la quantité des paquets de données transmis et réceptionnés via les connexions réseau sont souvent collectées pour des raisons commerciales. Pour les fournisseurs d'accès Internet facturant leur clients par volume de données, cette opération est essentielle.

Toutefois, la comptabilité réseau détaillée présente de nombreux avantages, qui ne se limitent pas aux fins commerciales. Si par ex. vous gérez un serveur qui offre différents types de services réseau, il vous est utile de savoir combien de données sont générées par les différents services.

Votre appareil comprend la fonction de comptabilité IP, qui vous permet de collecter de multiples informations utiles au sujet du trafic réseau IP (chaque session IP individuelle).

17.2.1 Interfaces

Dans ce menu, vous pouvez configurer la fonction de comptabilité IP pour chaque interface individuelle.

Le menu **Création de rapports externe**->**IP-Accounting**->**Interfaces** contient la liste de toutes les interfaces configurées sur votre appareil. La fonction de comptabilité IP peut être activée pour chaque entrée en cochant la case correspondante. Dans la colonne **IP-Accounting**, vous n'avez pas besoin de cliquer sur chaque entrée individuelle. L'option **Sélectionner tout** ou **Désactiver tout** vous permet d'activer ou de désactiver la fonction de comptabilité IP simultanément pour toutes les interfaces.

17.2.2 Options

Ce menu vous permet de configurer les paramètres généraux pour la comptabilité IP.

Le menu **Création de rapports externe**->**IP-Accounting**->**Options** vous permet de définir le **Format de journal** des messages de comptabilité IP. Les messages peuvent contenir des chaînes de caractères dans un ordre quelconque, des séquences séparées par des antislash, par ex. `\t` ou `\n` ou des tags définis.

Tags de formats possibles :

Tags de formats pour messages IP-Accounting.

Champ	Description
%d	Date du début de session au format JJ.MM.AA.
%t	Heure de début de session au format HH:MM:SS.
%a	Durée de la session en secondes
%c	Protocole
%i	Adresse IP source
%r	Port source
%f	Indice d'interface source
%I	Adresse IP cible
%R	Port cible
%F	Indice d'interface cible
%p	Paquets sortants
%o	Octets sortants
%P	Paquets entrants

Champ	Description
%O	Octets entrants
%s	N° d'ordre du message d'enregistrement de frais
%%	%

Par défaut, le champ **Format de journal** contient l'instruction de format suivante : *INET: %d%t%a%c%i:%r/%f -> %I:%R/%F%p%o%P%O[%s]*

17.3 Service de notification

Jusqu'à présent, il était déjà possible de faire transmettre des messages syslog du routeur à un hôte syslog quelconque. Grâce au service de notification, l'administrateur reçoit, en fonction de la configuration, des e-mails dès l'apparition de messages syslog pertinents.

17.3.1 Destinataire de la notification

Le menu **Destinataire de la notification** affiche la liste de tous les messages syslog.

17.3.1.1 Nouveau

Actionnez le bouton **Nouveau** pour créer d'autres destinataires de notifications supplémentaires.

Le menu **Création de rapports externe**->**Service de notification**->**Destinataire de la notification**->**Nouveau** se compose des champs suivants :

Champs du menu Ajouter/éditer le destinataire de la notification

Champ	Description
Service de notification	Permet d'afficher le service de notification.
Destinataire	Saisissez l'adresse e-mail ou le numéro du téléphone portable du destinataire. La saisie est limitée à 40 caractères.
Compression des messages	Indiquez si le texte de l'e-mail de notification doit être abrégé. L'e-mail contient alors une seule occurrence du message syslog, ainsi que le nombre d'événements correspondants. Activez ou désactivez le champ. La fonction est activée par défaut.

Champ	Description
Objet	Vous pouvez saisir un objet.
Evénement Trigger Add/Edit	Cette fonction n'est disponible que sur les appareils équipés d'un contrôleur LAN sans fil. Choisissez l'événement qui doit déclencher une notification par e-mail. Valeurs possibles : • *Le message système contient une chaîne de caractères* (valeur par défaut) : Un message syslog contient une séquence de caractères définie.
Chaîne de caractères correspondants	Vous devez saisir une « Séquence de caractères contenue ». Sa présence d'un un message syslog constitue la condition préalable pour le déclenchement d'une alarme. La saisie est limitée à 55 caractères. Veuillez noter que sans l'utilisation de caractères de substitution (par ex. « * »), seuls les chaînes de caractères correspondant exactement à la saisie remplissent la condition. Généralement, la « séquence de caractères contenue » saisie comprendra donc aussi des caractères de substitution. Pour être informé systématiquement de tous les messages syslog du niveau sélectionné, il convient de ne saisir que « * ».
Degré de sévérité	Sélectionnez le degré de gravité dans lequel la chaîne de caractères configurée dans le champ **Chaîne de caractères correspondants** doit être incluse afin de déclencher une notification par e-mail. Valeurs possibles : *Urgence* (Valeur par défaut), *Alarme*, *Critique*, *Erreur*, *Avertissement !*, *Notification*, *Informations*, *Debug*
Sous-systèmes surveillés	Sélectionnez les sous-systèmes à surveiller. Ajoutez de nouveaux sous-systèmes à l'aide de la fonction **Ajouter**.
Timeout pour les messages	Saisissez la durée d'attente maximale du routeur après un évé-

Champ	Description
	nement correspondant, avant que l'envoi des e-mails de notification ne soit forcé. Les valeurs comprises entre *0* et *86400* sont disponibles. Une valeur de *0* désactive le dépassement du temps imparti. La valeur par défaut est *60*.
Nombre de messages	Saisissez le nombre de messages syslog à atteindre avant qu'une notification par e-mail ne puisse être envoyée pour ce cas. Lorsque le dépassement du temps imparti est configuré, l'e-mail est envoyé après écoulement de ce temps, même si le nombre de messages n'est pas encore atteint. Les valeurs disponibles s'étendent de *0* à *99*, la valeur par défaut étant de *1*.

17.3.2 Paramètres de notification

Le menu **Création de rapports externe**->**Service de notification**->**Paramètres de notification** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Service de notification	Indiquez si le service de notification doit être activé. Sélectionnez *Activé* pour activer la fonction. La fonction est activée par défaut.
Nombre maximal d'e-mail par minute	Limitez le nombre d'e-mails envoyés par minute. Les valeurs disponibles s'étendent de *1* à *15*, la valeur par défaut étant de *6*.

Champs du menu Paramètres e-mail

Champ	Description
Adresse e-mail de l'expéditeur	Saisissez l'adresse e-mail à entrer dans le champ de l'émetteur de l'e-mail.
Serveur SMTP	Saisissez l'adresse (adresse IP ou nom DNs valide) du serveur de messagerie qui doit être utilisé pour l'envoi des e-mails.

Champ	Description
	La saisie est limitée à 40 caractères.
Authentification SMTP	Authentification attendue par le serveur SMTP. Valeurs possibles : • *aucun* (valeur par défaut) : Le serveur accepte et envoie les e-mails sans autre authentification. • *ESMTP*: Le serveur n'accepte les e-mails que si le routeur le connecte avec la combinaison de nom d'utilisateur/mot de passe correct. • *SMTP after POP*: Le serveur exige qu'avant l'envoi d'un e-mail, les e-mails soient lus via POP3 depuis l'IP expéditrice avec le nom d'utilisateur/mot de passe POP3 correct.
Nom de l'utilisateur	Uniquement si **Authentification SMTP** = *ESMTP* ou *SMTP after POP* Indiquez le nom d'utilisateur pour le serveur POP3 et/ou SMTP.
Mot de passe	Uniquement si **Authentification SMTP** = *ESMTP* ou *SMTP after POP* Indiquez le mot de passe de cet utilisateur.
Serveur POP3	Uniquement si **Authentification SMTP** = *SMTP after POP* Saisissez l'adresse du serveur qui doit lire les e-mails.
Timeout POP3	Uniquement si **Authentification SMTP** = *SMTP after POP* Saisissez la durée d'attente maximale du routeur après la lecture POP3, avant que l'envoi des e-mails d'alerte ne soit forcé. La valeur par défaut est *600* secondes.

Erreur dans le menu Paramètres SMS (uniquement sur RS120wu, RS230au+ et RS230bu+).

Champ	Description
Appareil SMS	Vous pouvez vous laisser notifier par SMS des messages système. Sélectionnez l'appareil à utiliser pour l'envoi des SMS.

Champ	Description
SMS maxi par jour	Limitez ici le nombre des SMs envoyés par jour. L'activation de *Illimité* permet d'envoyer un nombre illimité de SMS. La valeur par défaut est de 10 SMS par jour. Remarque : La saisie de la valeur 0 correspond à l'activation de *Illimité*.

17.4 SNMP

SNMP (Simple Network Management Protocol) est un protocole de la famille de protocoles IP destiné au transport d'informations de gestion au sujet des éléments de réseau.

Parmi les éléments de chaque système de gestion SNMP figure notamment une MIB. SNMP permet de configurer, de piloter et de surveiller différents éléments de réseau depuis un seul système. Avec votre appareil, vous avez obtenu un tel outil SNMP, le gestionnaire de configuration. Comme SNMP est un protocole normalisé, vous pouvez aussi utiliser un autre gestionnaire SNMP quelconque, par ex. HPOpenView.

Vous trouverez des informations complémentaires au sujet des versions SNMP dans les RFC et ébauches correspondantes :

- SNMP V. 1 : RFC 1157
- SNMP V. 2c : RFC 1901 - 1908
- SNMP V. 3 : RFC 3410 - 3418

17.4.1 Options SNMP-Trap

Pour surveiller le système, un message est envoyé en cas de dysfonctionnement, appelé paquet Trap.

Le menu **Création de rapports externe**->**SNMP**->**Options SNMP-Trap** vous permet de configurer l'envoi des Traps.

Le menu **Création de rapports externe**->**SNMP**->**Options SNMP-Trap** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
SNMP Trap Broadcasting	Indiquez si le transfert de Traps SNMP doit être activé. Votre appareil transmet alors les Traps SNMP à l'aidresse de diffusion du LAN. Sélectionnez *Activé* pour activer la fonction. La fonction est désactivée par défaut.
Port SNMP-Trap-UDP	Uniquement si **SNMP Trap Broadcasting** est activé. Saisissez le numéro du port UDP vers lequel votre appareil doit envoyer des Traps SNMP. Toute valeur entière est possible. La valeur par défaut est *162*.
SNMP-Trap-Community	Uniquement si **SNMP Trap Broadcasting** est activé. Saisissez un identifiant SNMP. Celui-ci doit être transmis par le gestionnaire SNMP avec chaque demande de SNMP, afin qu'elle soit acceptée par votre appareil. Une chaîne de *0* à *255* caractères est possible. La valeur par défaut est *Trap SNMP*.

17.4.2 SNMP-Trap-Hosts

Ce menu vous permet d'indiquer les adresses IP vers lesquelles votre appareil doit envoyer les Traps SNMP.

Le menu **Création de rapports externe**->**SNMP**->**SNMP-Trap-Hosts** contient la liste de tous les hôtes de Traps SNMP configurés.

17.4.2.1 Nouveau

Actionnez le bouton **Nouveau** pour configurer d'autres hôtes de Traps SNMP.

Le menu **Création de rapports externe**->**SNMP**->**SNMP-Trap-Hosts**->**Nouveau** se compose des champs suivants :

Champs du menu Paramètres de base

Champ	Description
Adresse IP	Saisissez l'adresse IP de l'hôte de Traps SNMP.

Chapitre 18 Monitoring

Ce menu contient des informations permettant de déceler des problèmes dans votre réseau et de surveiller les activités, par ex. au niveau de l'interface WAN de votre appareil.

18.1 Information d'état

Ce menu sert à visualiser les paramètres actuels des terminaux et des abonnés de l'équipe. Ces informations sont extraites en continu.

18.1.1 Utilisateur

Le menu **Monitoring**->**Information d'état**->**Utilisateur** affiche les paramètres actuels du numéro d'appel interne (MSN) d'un utilisateur.

L'actionnement du bouton affiche des statistiques détaillées concernant l'utilisateur respectif.

Valeurs de la liste Etat de l'abonné

Champ	Description
Numéro d'appel (MSN)	Permet d'afficher le numéro d'appel interne de l'utilisateur.
Nom	Indique le nom attribué à l'utilisateur. Si un système Voice Mail est actif, *Système boîte vocale* s'affiche.
Classe d'autorisation actuelle	Indique toutes les classes d'autorisation affectées à l'utilisateur. La classe d'autorisation active actuelle est identifiée par une flèche verte ( ).
Appareil terminal	Indique l'interface à laquelle l'abonné est affecté.
Coûts	Indique les coûts calculés pour les unités de connexion consommées.
État	Indique l'état de l'interface à laquelle l'abonné est connecté.

Valeurs de la liste Réglage système

Champ	Description
Appel en parallèle	Indique si l'appel en parallèle est configuré pour l'utilisateur.
Transfert des appels	Indique le transfert d'appels activé actuellement pour cet utili-

Champ	Description
(AWS)	sateur.
Protection d'appel (silence)	Indique si la protection de signal d'appel est configurée pour l'utilisateur. (Uniquement pour les téléphones système)
Signal appel en attente	Indique si un signal d'appel peut être indiqué pour les appels internes et/ou externes.
Appel direct	Indique si l'appel direct après décrochage du combiné est configuré pour l'utilisateur.
Surveillance de la pièce	Indique si la surveillance du local est activée pour l'utilisateur.
Annonce	Indique si l'annonce est autorisée pour l'utilisateur.
Interphone	Indique si l'interphonie est autorisée pour l'utilisateur.
Prise d'appel automatique	Indique si la prise d'appels automatique est configurée pour l'utilisateur.

18.1.2 Teams

Le menu **Monitoring**->**Informations d'état**->**Equipes** affiche les paramètres actuels pour les équipes.

L'actionnement du bouton affiche des statistiques détaillées concernant l'équipe respective.

Valeurs de la liste Etat Team

Champ	Description
Nom	Indique le nom attribué à l'équipe.
Numéro d'appel (MSN)	Permet d'afficher le numéro d'appel interne de l'équipe.
Utilisateurs affectés/ Utilisateurs connectés	Indique les utilisateurs affectés à l'équipe et le nombre connecté de ces utilisateurs.
Transfert des appels (AWS)	Indique le transfert d'appels activé actuellement pour cette équipe.

Valeurs de la liste Réglage système

Champ	Description
Variante active (jour)	Indique la variante d'appel activée actuellement pour cette équipe.
Commuter la variante d'appel	Indique si la variante d'appel manuel, par calendrier ou manuel et par calendrier peut être commutée.

Champ	Description
Signaler	Indique le type de signalement d'appels dans l'équipe.
Occupé par occupé (Busy on Busy)	Indique si Occupé pour Occupé est configuré pour l'équipe.
Prise d'appel automatique	Indique si la prise d'appels automatique est configurée et quelle musique d'attente est sélectionnée.
Rejet en absence de réponse	Indique si le transfert en absence de réponse est activé et après combien de temps le transfert est réalisé vers quelle équipe.
Autres fonctions de rejet	Indique lesquelles des fonctions de transfert sont activées et vers quel abonné les appels sont transférés.

Le menu **Paramètres étendus** se compose des champs suivants :

Valeurs de la liste Paramètres étendus

Champ	Description
Utilisateurs affectés	Indique tous les abonnés connectés et déconnectés de l'équipe.

18.2 Journal interne

18.2.1 Messages système

Le menu **Monitoring**->**Journal interne**->**Messages système** contient la liste de toutes les messages système enregistrés en interne. Au-dessus du tableau se toruvent les valeurs configurées pour les champs **Nombre maximal d'entrées de journal Syslog** et **Niveau maximal de messages des entrées de journal système**. Ces valeurs peuvent être modifiées dans le menu **Gestion du système**->**Paramètres globaux**->**Système**.

Valeurs de la liste Messages système

Champ	Description
N°	Indique le numéro d'ordre du message système.
Date	Indique la date de l'enregistrement.
Heure	Indique l'heure de l'enregistrement.
Niveau	Indique le classement hiérarchique du message.
Sous-système	Indique le sous-système de votre appareil ayant généré le message.
Message	Affiche le texte du message.

18.3 IPSec

18.3.1 Tunnel IPSec

Le menu **Monitoring**->**IPSec**->**Tunnel IPSec** affiche la liste de tous les tunnels IPSec configurées.

Valeurs de la liste Tunnel IPSec

Champ	Description
Description	Affiche le nom de la connexion IPSec.
Adresse IP distante	Affiche l'adresse IP du pair IPSec distant.
Réseaux distants	Affiche les sous-réseaux actuellement convenus par le dispositif.
Algorithme de sécurité	Affiche l'algorithme de cryptage de la connexion IPSec.
État	Affiche l'état de service de la connexion IPSec.
Action	Permet de modifier l'état de la connexion IPSec comme indiqué.
Détails	Ouvre une fenêtre de statistiques détaillées.

Le statut de la connexion IPSec est modifié en actionnant le bouton ou le bouton dans la colonne **Action**.

L'actionnement du bouton affiche des statistiques détaillées concernant la connexion IPSec respective.

Valeurs de la liste Tunnel IPSec

Champ	Description
Description	Affiche la description du pair.
Adresse IP locale	Affiche l'adresse IP WAN de votre appareil.
Adresse IP distante	Affiche l'adresse IP WAN du partenaire de communication.
ID locale	Affiche l'identifiant de votre appareil pour cette connexion IPSec.
ID distante	Affiche l'identifiant du pair.
Mode négociation	Affiche le mode de négociation.
Méthode d'authentification	Affiche la méthode d'authentification.

Champ	Description
MTU	Affiche la MTU (Maximum Transfert Unit) actuelle.
Contrôle d'accessibilité	Affiche la méthode de contrôle de joignabilité du pair.
Détection NAT	Affiche la méthode de reconnaissance NAT.
Port local	Affiche le port local.
Port distant	Affiche le port distant.
Paquets	Affiche le nombre de paquets entrants et sortants.
Octets	Affiche le nombre d'octets entrants et sortants.
Erreur	Affiche le nombre d'erreurs.
IKE (Phase-1) SAs (x) **Rôle** / **Algorithme** / **Durée de vie restante** / **État**	Affiche les paramètres des SA IKE (phase 1).
IPSec (Phase-2) SAs (x) **Rôle** / **Algorithme** / **Durée de vie restante** / **État**	Affiche les paramètres des SA IPSec (phase 2).
Messages	Affiche les messages systèmes pour ce tunnel IPSec.

18.3.2 Statistiques IPSec

Dans le menu **Monitoring**->**IPSec**->**Statistiques IPSec** des valeurs statistiques pour toutes les connexions IPSec s'affichent.

Le menu **Monitoring**->**IPSec**->**Statistiques IPSec** se compose des champs suivants :

Champ du menu Licences

Champ	Description
Tunnel IPSec	Affiche le nombre de licences IPSec utilisées actuellement (**en service**) et le nombre de licences maximal utilisable (**Maximal**).

Champ du menu Peers

Champ	Description
État	Affiche le nombre de connexions IPSec comptées selon leur état actuel. • **Actif**: Connexions IPSec actives actuelles. • **Activer**: Connexions IPSec actuellement en cours de phase de constitution de tunnel. • **Bloqué**: Connexions IPSec bloquées. • **En veille**: Connexions IPSec inactives actuelles. • **Configuré**: Connexions IPSec configurées.

Champs du menu SAs

Champ	Description
IKE (Phase-1)	Permet d'afficher le nombre de Phase-1-SAs actifs (**Etabli**) par rapport au nombre total de Phase-1-SAs (**Total**).
IPSec (Phase-2)	Permet d'afficher le nombre de Phase-2-SAs actifs (**Etabli**) par rapport au nombre total de Phase-2-SAs (**Total**).

Champs du menu Statistiques du paquet

Champ	Description
Total	Affiche le nombre de tous les paquets entrants (**Entrant**) et sortants (**Sortant**) traités.
Transmis	Affiche le nombre de paquets entrants (**Entrant**) ou sortants (**Sortant**) qui ont été transmis en texte clair.
Rejeté	Affiche le nombre des paquets entrants (**Entrant**) et sortants (**Sortant**) rejetés.
Crypté	Affiche le nombre des paquets entrants (**Entrant**) et sortants (**Sortant**) protégés par IPSec.
Erreur	Affiche le nombre des paquets entrants (**Entrant**) et sortants (**Sortant**) lors du traitement desquels des erreurs sont apparues.

18.4 Interfaces

18.4.1 Statistiques

Le menu **Monitoring**->**Interfaces**->**Statistiques** affiche les valeurs et activités actuelles de toutes les interfaces d'appareils.

La barre de filtre vous permet de choisir si le **Transfert total** ou le **Débit de transfert** doit être affiché. La fenêtre **Débit de transfert** affiche les valeurs par seconde.

Le statut de l'interface est modifié en actionnant le bouton ou le bouton dans la colonne **Action**.

Valeurs de la liste Statistiques

Champ	Description
N°	Indique le numéro d'ordre de l'interface.
Description	Permet d'afficher le nom de l'interface.
Type	Permet d'afficher le type d'interface.
Paquets Tx	Permet d'afficher le nombre total de paquets envoyés.
Octets Tx	Permet d'afficher le nombre total d'octets envoyés.
Erreur Tx	Permet d'afficher le nombre total d'erreurs envoyées.
Paquets Rx	Permet d'afficher le nombre total de paquets reçus.
Octets Rx	Permet d'afficher le nombre total d'octets reçus.
Erreur Rx	Permet d'afficher le nombre total d'erreurs reçues.
État	Permet d'afficher l'état de fonctionnement de l'interface sélectionnée.
Non modifié depuis	Permet d'afficher la durée depuis laquelle l'état de fonctionnement de l'interface n'a pas changé.
Action	Permet de modifier l'état de l'interface comme indiqué.

Le bouton permet d'afficher les données statistiques détaillées pour les interfaces individuelles.

Valeurs de la liste Statistiques

Champ	Description
Description	Permet d'afficher le nom de l'interface.
Adresse MAC	Permet d'afficher le type d'interface.
Adresse IP/Masque de réseau	Affiche l'adresse IP et le masque de réseau.
NAT	Permet d'afficher si NAT est activé pour cette interface.
Paquets Tx	Permet d'afficher le nombre total de paquets envoyés.
Octets Tx	Permet d'afficher le nombre total d'octets envoyés.
Paquets Rx	Permet d'afficher le nombre total de paquets reçus.

Champ	Description
Octets Rx	Permet d'afficher le nombre total d'octets reçus.

Champ du menu Connexions TCP

Champ	Description
État	Permet d'afficher l'état d'une connexion TCP active.
Adresse locale	Permet d'afficher l'adresse IP locale de l'interface pour une connexion TCP active.
Port local	Permet d'afficher le port local de l'adresse IP pour une connexion TCP active.
Adresse distante	Permet d'afficher l'adresse IP avec laquelle une connexion TCP active est établie.
Port distant	Permet d'afficher le port avec lequel une connexion TCP active est établie.

18.5 Passerelle hotspot

18.5.1 Passerelle hotspot

Le menu **Monitoring**->**Passerelle hotspot**->**Passerelle hotspot** affiche la liste de tous les utilisateurs de Hotspot connectés.

Valeurs de la liste Passerelle hotspot

Champ	Description
Nom de l'utilisateur	Permet d'afficher le nom de l'utilisateur.
Adresse IP	Permet d'afficher l'adresse IP de l'utilisateur.
Adresse physique	Permet d'afficher l'adresse physique de l'utilisateur.
Connexion	Permet d'afficher le moment de la connexion.
Interface	Permet d'afficher l'interface utilisée.

18.6 QoS

Le menu **Monitoring**->**QoS** affiche les statistiques pour les interfaces pour lesquelles QoS a été configuré.

18.6.1 QoS

Le menu **Monitoring**->**QoS**->**QoS** affiche la liste de toutes les interfaces pour lesquelles QoS a été configuré.

Valeurs de la liste QoS

Champ	Description
Interface	Permet d'afficher l'interface pour laquelle QoS a été configurée.
Queue QoS	Permet d'afficher la queue QoS qui a été configurée pour cette interface.
Envoyer	Permet d'afficher le nombre de paquets envoyés avec la classe de paquets correspondante.
Rejeté	Permet d'afficher le nombre de paquets rejetés avec la classe de paquets correspondante en cas de surcharge.
Queued	Permet d'afficher le nombre de paquets en attente avec la classe de paquets correspondante en cas de surcharge.

Index

#1 #2, #3 50
Accepter les appel en attente avect 158
Accès 365
Accès personnel 94
Action 238 , 333 , 372 , 400
Action à exécuter 385
Action de l'interface 387
Activé 328
Activer la mise à jour 355
Adresse du serveur 372
Adresse e-mail 89
Adresse e-mail (provenant des paramètres utilisateur) 189
Adresse GRE-IP distante 328
Adresse GRE-IP locale 328
Adresse groupes multicast 249
Adresse IP 350 , 363 , 415 , 423
Adresse IP locale 240
Adresse IP de destination/Masque de réseau 205 , 214 , 219 , 234 , 282 , 397
Adresse IP de destination 367 , 372 , 388
Adresse IP de la passerelle 205
Adresse IP distante 311
Adresse IP du serveur 32 , 36
Adresse IP du client SIP 134
Adresse IP locale 205 , 256 , 260 , 265 , 279 , 312 , 315 , 321 , 328
Adresse IP source 367 , 372 , 385 , 388
Adresse IP source publique 285
Adresse IP source/Masque de réseau 206 , 214 , 219 , 234 , 282 , 397
Adresse IP surveillée 385
Adresse IP/Masque de réseau 197
Adresse MAC 125 , 129 , 197 , 363
Adresse MAC cible 400
Adresse MAC DHCP 198
Adresse Peer 277
Adresse PPTP-IP distante 261 , 320
Adresse PPTP-IP distante Nom de l'hôte 320
Adresse PPTP-IP locale 261
Adresse réseau 240
Adresse/Sous-réseau 339
Adresses 73
Affectation 115 , 120 , 163 , 182
Affectation externe 115 , 182
Affectation interne 87 , 115 , 182 , 187
Affectation pour rejet et tarifs 115
Afficher la date et l'heure 138
Afficher le numéro d'appel de l'interlocuteur distant 65 , 81
Afficher le nom entrant (CNIP) 138
Afficher le numéro d'appel fixe pour les communications sortantes 65 , 81
Afficher le numéro d'appel (CLIP) 138
Afficher le numéro d'appel entrant (CLIP-Offhook) 138
Afficher les nouveaux messages (MWI) 139
Algorithme Dropping 231
Algorithme de priorétisation 225
Annonce 159
Annonce 109
Annonce avant interrogation avec DISA 161
Appareil en amont avec NAT 68
Appel en parallèle 112
Appel en parallèle après le temps 114 , 182
Application 154
Application du rejet 93 , 121
Appliquer QoS 333
ARP Lifetime 240
Arrêt dans le système 68 , 82
Attribution des adresses IP 279
Authentification 257 , 261 , 266 , 316 , 322
Autorisation d'accès 122

Autorisation de numérotation 96
Autorisation TFE 110
Autoriser groupage manuel 96
Autoriser la connexion d'un proxy 68
Autoriser le transfert des appels 113
Autoriser les connexions multiples 135
Autres fonctions de rejet 119 , 176
Bande passante maximale en descente 73
Bande passante montante maximale 73
Basculer vers le navigateur SNMP 40
Bloquer après erreur de connexion pour 257 , 261 , 266 , 316 , 322
Calendrier pour état "en extérieur" 189 , 191
Call Through 95 , 103 , 167
Callback 325
Certificat d'encryptage RA 46
Certificat CA 46
Certificat de signature RA 46
Certificat local 292
Certificat surveillé 367
Certificats CA 297
Chaîne de caractères correspondants 418
Chaîne de règle 238 , 239 , 402
Chaîne de règles Wake-On-LAN 400
Champs d'en-tête SIP pour adresse d'appel 68
Champs d'en-tête SIP pour le nom d'utilisateur 68
Chemin d'accès URL LDAP 53
Chemin de mise à jour 357
Classe High-Priority 222
Classe de routes 203
Classe numéro 40
Clé de licence 20
Client DHCP sur l'interfaces 240
Client hotspot admis. 395
CLIP 61
Code 341
Code acceptation TFE 180
Code sonnerie 181
Commuter la variante 181 , 184
Commuter la variante d'appel 113 , 162 , 175
Commuter les variantes d'appel manuellement 103
Compression 322
Compression des messages 418
Compression IP 302
Condition de comparaison 367
Condition de trafic de l'interface 367
Condition horaire 371
Condition pour la liste d'événements 372
Conditions de vente 393
Configuration réseau 240
Connexion de l'installation MSN supplémentaire 84
Connexion externe 84 , 120 , 123
Contact relais 185
Contrôle d'accessibilité 34 , 297 , 302
Contrôle d'accessibilité LCP 257 , 261 , 316 , 322
Contrôle de la version 372
Contrôle de numérotation 99
Couche 1 synchronisation permanente 58
Création entrée NAT 256 , 260 , 265 , 315 , 321
Créer un numéro d'appel international 68
Créer un numéro d'appel national 68
Cryptage 37 , 266 , 316 , 322
Crypter la configuration 372
Date (JJ-MM) 157
Définir l'état de l'interface 372
Définir la valeur COS (802.1p/couche 2) 222
Définir la valeur DSCP/TOS (couche 3) 222
Degré de sévérité 418
Désactiver la désactivation du numéro 68

Description 40 , 44 , 53 , 57 , 61 , 65 , 73 , 76 , 80 , 86 , 88 , 96 , 113 , 125 , 129 , 133 , 136 , 137 , 141 , 144 , 148 , 150 , 151 , 154 , 157 , 158 , 162 , 165 , 167 , 175 , 181 , 184 , 206 , 212 , 219 , 222 , 229 , 234 , 238 , 254 , 259 , 264 , 277 , 282 , 292 , 299 , 304 , 310 , 313 , 320 , 328 , 339 , 339 , 340 , 341 , 343 , 348 , 363 , 367 , 372 , 397 , 400
Description affichée 91 , 93 , 127 , 131
Description de certificat locale 51 , 52 , 372
Description de la demande de certificat 46 , 372
Description du groupe 32 , 240
Description du centre d'appel 175
Destinataire 418
Destination 333
Détection de la sonnerie occupé 62
Détection de la sonnerie de numérotation 62
Deuxième numéro d'appel externe 187
DHCP Broadcast Flag 198
Directive 34 , 37
Domaine 65 , 351
Domaine sur le serveur hotspot 393
DTMF 76
Durée d'enregistrement maxi 189
Durée de validité restante 367
Durée de vie 292 , 299
E-mail 48
Echange de données transmis 367
Ecraser certificat similaire 372
Ecrire le certificat dans la configuration 372
Emplacement 68 , 125 , 129 , 133
Emplacement contenant (parent) 73
Encodage du fichier 51 , 52
Enregistrer la configuration 40
Enregistrer les données de connexion 110
Entrée active 32 , 36
Entrées 270
Entrées de route 256 , 260 , 265 , 279 , 315 , 321 , 328
État 120 , 177 , 184 , 187 , 367
État administratif 277 , 348
Etat de l'interface 367
Etat de la connexion 219 , 234 , 397
Etat de la zone GEO 367
État du déclencheur 372
État du fournisseur 65
État du propriétaire de la boîte mail 191
Etat/Province 48
Evénement Trigger Add/Edit 418
Evitement de goulet d'étranglement (RED) 231
Exception numérotation directe (P-P) 84
Exclure du NAT (DMZ) 240
Facility 415
Fenêtre de connexion 395
Fenêtre pop-up pour affichage de l'état 395
Fichier wave 185
Filtre 222
Filtre COS (802.1p/Layer 2) 219 , 234 , 397
Filtre d'accès 238
Filtre DSCP/TOS (couche 3) 219 , 234 , 397
Filtre Wake-On-LAN 400
Filtres supplémentaires du trafic de données 281 , 282
Fonction de rejet 176
Forcer la fiabilité du certificat 44
Format de fichier CSV 372
Fournisseur sans enregistrement 68
From Domain 68
G.711 aLaw 76
G.711 uLaw 76
G.722 76
G.726 (16 Kbits/s) 76

G.726 (24 Kbits/s) 76
G.726 (32 Kbits/s) 76
G.726 (40 Kbits/s) 76
G.729 76
Générer une clé privée 46
Groupage des canaux 269
Groupe DH 292
Groupe Pick-Up 103
Heure de début 371
Heure de reroutage en cas d'absence de réponse 159
Horloge d'enregistrement 67
Horloge de surveillance de fin de numérotation 68
Horloger de connexion externe 185
Horodatage 415
Hôte 351
ID d'authentification 65
ID de classe 222 , 229
ID de groupes 384
ID groupe serveur RADIUS 304
ID locale 277
ID Peer 277
ID VLAN 197 , 254
Identifiant VLAN 201
IGMP Proxy 247
IKE (Internet Key Exchange) 277
Immédiatement 119
Indicatif fournisseur 150
Informations supplémentaires sur l'appel externe 99
Interface 25 , 26 , 136 , 137 , 180 , 184 , 203 , 212 , 225 , 239 , 246 , 273 , 336 , 348 , 351 , 355 , 359 , 372 , 387 , 393 , 402
Interface surveillée 367
Interface de destination 249
Interface Ethernet-PPPoE 254
Interface Ethernet-PPTP 259
interface PPPoE pour liaison multiple 254
Interface proxy 247
Interface sortante 229
Interface source 206 , 249
Interface surveillée 387
Interfaces 73 , 222
Intervalle 367 , 372 , 385 , 388
Intervalle d'interrogation 246
Intervalle de mise à jour 357
Intervalle de réponse (dernier membre) 246
Intervalle Hello 312
Journal 214 , 219 , 234 , 282 , 341 , 357 , 372 , 397 , 415
L'utilisateur doit changer le mot de passe 42
La configuration contient des certificats/clés 372
Langue Boîte vocale 189
Langue pour fenêtre de connexion 393
Le certificat est un certificat CA 44
Lease Time 360
Liaison IP/MAC 125 , 129
Lieu 48
Ligne extérieure automatique 96
Limitation de la bande passante en descente 73
Limitation de la bande passante en montée 73
Liste des événements 367 , 372
Mail-Exchanger (MX) 356
Maintenir le niveau 2 actif en permanence 58
Masque réseau 240 , 315
Membres 339 , 343
Membres VLAN 201
Message d'information (UUS1) 185
Méthode d'authentification 277 , 292
Méthode de compte-rendu 239
Méthode de numérotation 61
Méthode NAT 212
Métrique 205 , 279
MobIKE 285
Mode 46 , 206 , 240 , 246 , 270 , 289 , 292 , 304
Mode Adresse IP 256 , 260 , 265 , 315 , 321

Mode adresse PPTP 261
Mode adresses 197
Mode Callback 266
Mode client SIP 134
Mode d'instruction 372
Mode de fonctionnement (Actif) 372
Mode de fonctionnement (Inactif) 372
Mode de transmission 289
mode de configuration 279
Mode de contrôle 225 , 273
Mode de l'exploitant 32
Mode de routage 150
Mode démarrage 283
Mode du canal D 289
Mode enregistrement automatique 50 , 372
Mode interfaces 197 , 348
Mode OSPF 270 , 317 , 324
Mode pour état "Au bureau" 191
Mode PPPoE 254
Mode PPTP 320
Mode Proxy ARP 270 , 317 , 324
Mode RTT (Realtime-Traffic-Modus) 229
Mot de passe 42 , 46 , 51 , 52 , 65 , 94 , 254 , 259 , 264 , 304 , 310 , 313 , 320 , 355 , 365 , 372 , 400
Mot de passe RADIUS 32
Mot de passe administrateur 128 , 132
Mot de passe pour certificat protégé 372
Mot de passe pour enregistrement téléphonique IP 94
Mot de passe TACACS+ 36
Mot de passe utilisateur par défaut 32
MTU 328
Musique d'attente (MoH) 110
NAT-Traversal 297
Négociation DNS 257 , 261 , 270 , 317 , 324
Net Direct (Keypad) 109
Niveau 415
Niveau d'accès 42
Niveau de routage 1 151
Niveau de routage 2 151
Nom 57 , 61 , 88 , 304
Nom affiché 84
Nom CA 372
Nom d'hôte distant 310
Nom d'hôte DHCP 198
Nom d'hôte DNS 350
Nom d'hôte local 310
Nom de fichier externe 51 , 52
Nom de fichier local 372
Nom de l'hôte 355
Nom de l'objet 372
Nom de l'utilisateur 65 , 94 , 254 , 259 , 264 , 313 , 320 , 355 , 365
Nom de la sonnerie 181
Nom de pool IP 272 , 306 , 327 , 359 , 359
Nom du fichier 372
Nom du fichier dans flash 372
Nom du fichier sur le serveur 372
Nom du fournisseur 357
Nom général 48
Nom VLAN 201
Nombre d'abonnés dans la boucle d'attente 158
Nombre d'émissions 161 , 185
Nombre de communications simultanées admises 68
Nombre de répétitions 185
Nombre de connexions autorisées 283
Nombre de messages 418
Nombre de ports utilisés 270
Nombre maximal de tentative de composition du numéro 257 , 261 , 266
Nombre maximal de répétitions 312
Nombre maximal de messages d'état IGMP 246
Noms de domaines supplémentaires à accès libre 393
Notification par e-mail 189

Nouveau port de destination 217
Nouveau port source 217
Nouvelle adresse IP source/Masque de réseau 217
Nouvelle adresse IP de destination/ Masque de réseau 217
Nuit 89
Numéro d'appel 270
Numéro d'appel bloqué 147
Numéro d'appel direct 144
Numéro d'appel entrant 289
Numéro d'appel externe 112 , 175
Numéro d'appel interne 91 , 93 , 112 , 113 , 121 , 127 , 137 , 146 , 175 , 178 , 180 , 184 , 189
Numéro d'appel sortant 65 , 81 , 91 , 289
Numéro d'appel activé 147
Numéro d'appel Connexion de l'installation 84
Numéro d'appel de destination 159
Numéro d'appel de destination "en absence de réponse" 146
Numéro d'appel de destination "immédiatement" 146
Numéro d'appel de destination "si occupé" 146
Numéro d'appel global pour CLIP-No-Screening 65 , 81
Numéro d'appel interne 131
Numéro d'appel privé 89
Numéro d'appel unique (MSN) 84
Numéro de mobile 89 , 131
Numéro de port 134
Numéro de série de la licence 20
Numéro de téléphone 167
Numéro prioritaire 148
Numéro RNIS entrant 325
Numéro RNIS sortant 325
Numéros d'appel 120 , 177
Numéros d'appel internes 91 , 133 , 136 , 141
Numéros de séquence des paquets de données 312
Numérotation abrégée 167
N° de connexion 127
Objet 418
Occupation de la ligne avec indicatif 96
Occupé en commençant par 119
Occupé par occupé (Busy on Busy) 90 , 117
Occupé quand 176
Optionnel 89
Options DHCP 360
Ordre Codec 76
Ordre dans le groupage 86
Organisation 48
Par défaut 89
Paramètres Codec G.726 76
Paramètres DSCP pour données RTP 75
Paramètres numéro d'appel interne et rejet 122
Pas d'attente et récupération 126 , 130 , 135
Passerelle 360
Pause sonnerie de numérotation 62
Pays 48
Période de signalisation de l'alarme 185
Personnalisé 48
PIN (6 caractères) 122
PIN pour accès par téléphone 94
Plage d'adresses 339
Plage d'adresses IP 272 , 306 , 321 , 327 , 359
Plage de port source 341
Plage de port de destination 341
Plan de classe 222
Pondération 229
Pool d'affectation IP 265 , 279
Pool d'affectation IP (IPCP) 315 , 321
Port 80 , 357
Port de destination/zone 214 , 219 , 234 , 397
Port de destination 206 , 282
Port de destination UDP 311

Port Proxy 68
Port Registrar 66
Port serveur STUN 67
Port source 206 , 214 , 282
Port source UDP 311
Port source/zone 214 , 219 , 234 , 397
Port TCP 37
Port UDP 34
Ports 80
Ports sélectionnés 325
Ports spécifiques 325
Post-traitement 114 , 179
Premier numéro d'appel externe 187
Prendre en compte les jours fériés 156
Preshared Key 277
Priorétiser les paquets TCP ACK 257 , 261 , 316 , 322
Priorité 32 , 36 , 229 , 333 , 348
Priority Queueing 229
Prise d'appel automatique avec 117 , 176
Prise en charge Early-Media 68
Prise en charge T.38 FAX 68
Profil Codec 127 , 131 , 135
Profil de tunnel 313
Profil Phase-1 283
Profil Phase-2 283
Profil XAUTH 283
Profils Codec 68
Propagation PMTU 302
Proposals 292 , 299
Protection d'appel (silence) 138
Protocole transparent 66 , 68 , 134
Protocole couche 4 206
Provider 355
Provisioning-Server (code 3) 362
Proxy 68
Proxy ARP 198 , 285
Queues/Directives 225
RADIUS-Dialout 34
Real Time Jitter Control 225
Recevoir des communications inter-phone 109
Recevoir les informations MWI 109
Recevoir les informations sur les coûts 61
Redémarrage de l'appareil après 372
Redémarrer après exécution de la commande 372
Registrar 66
Règles de filtre 336
Règles de sélection (ARS) 99
Rejet en absence de réponse 119 , 176
Rejet sans notification 239
Rejet vers un numéro d'appel 123
Remplacement du préfixe du numéro entrant 68
Remplacer le préfixe international par "+" 68
Répéter vers 185
Répétitions 34
Réponse 350
Reprendre les paramètres de 155 , 156
Résumé 48
Rôle 304
Route 150
Route par défaut 256 , 260 , 265 , 279 , 315 , 321 , 328
Saisir la bande passante 336
Sélection 340
Sélection interfaces 240
Sélectionner fournisseur 362
Sélectionner interface 87
Sélectionner le fichier 165
Sélectionner les lignes 178
Sens 222
Sens de l'échange de données 367
Server Timeout 34
Serveur 357
Serveur DNS 272 , 306 , 327 , 351 , 359
Serveur DNS primaire 348
Serveur DNS secondaire 348
Serveur STUN 67

Service 214 , 219 , 234 , 333 , 397
Service de notification 418
Si occupé 119
Signal appel en attente 103 , 138
Signalisation 117 , 182
Solidité 246
Source 333 , 372
Sous-systèmes surveillés 418
Supprimer les liaisons SIP après le re-démarrage 68
Sur la base de l'interface Ethernet 197
Surréservation autorisée 229
Taille de l'en-tête du protocole sous la couche 3 225
Taille de la clé 372
Taille de la salve (burst) 229
Taille Max. Queue 231
Taille Min. Queue 231
TAPI 110
TCP-MSS-Clamping 198
Temps d'arrêt 371
Temps d'attente maxi dans la boucle d'attente 158
Temps de franchissement 114 , 176 , 182
Temps de blocage 37 , 297
Temps de commutation 155 , 156
Temps de réponse maximal 246
Temps de signalisation des appels 182
Temps de surveillance de fin de numérotation 62
Temps flash pour numérotation multi-fréquences 139
Temps maximal entre les tentatives 312
Temps minimal entre les tentatives 312
Tension alternative d'appel FXS 139
Tentatives 367 , 372 , 388
Tentatives échouées 385
Tentatives réussies 385
Terminal Endpoint Identifier (TEI) 87
Timeout 37
Timeout en cas d'inactivité 254 , 259 , 264 , 313 , 320
Timeout par défaut en cas d'inactivité 395
Timeout pour les messages 418
Toujours actif 254 , 259 , 264 , 313 , 320
Tous les groupes multicast 249
Traffic Shaping 229 , 336
Traffic Shaping 225
Transférer 351
Transférer à 351
Transfert des appels vers des numéros externes 113
Transmettre avec 159
Transmettre l'adresse IP propre par RNIS/GSM 289
Transmettre le numéro d'appel A (CLIP) 99
Transmettre le numéro d'appel B (COLP) 99
Transmettre les informations sur les coûts 139
Transmission 161
Transmission des coûts 110
Trigger 387
TTL 350
Type 73 , 219 , 234 , 341 , 397
Type d'adresse 339
Type d'appareil terminal 136 , 137
Type d'authentification 32 , 36
Type d'échange de données 212
Type d'événement 367
Type d'instruction 372
Type d'utilisation 266
Type de connexion 65
Type de connexion 57 , 60 , 80 , 264 , 313
Type de l'application de rejet 162
Type de la fonction de rejet 158
Type de la transmission de l'appel' 146
Type de message 415

Type de numéro d'appel 82 , 84
Type de routes 203
Type de téléphone 125 , 129
Type de ticket 395
Type ID local 277 , 292
Unité organisationnelle 48
URL du serveur 372
URL SCEP 46
URL serveur SCEP 372
URL Walled Garden 393
Utilisateur 42 , 127 , 131 , 178 , 304
Utilisateur distant (uniquement numérotation) 264
Utilisation du répertoire téléphonique du système 110
Utilisation pool 359
Utiliser CRL 372
Utiliser groupe PFS 299
Utiliser le rejet global 103
Valeur de comparaison 367
Valeur de la clé 328
Valeur DSCP/TOS 206
Valeur ID locale 292
Variable surveillée 367
Variables d'index 367 , 372
Variables MIB 372
Variables MIB/SNMP à ajouter/à éditer 372
Variante active (jour) 93 , 113 , 121
Variante d'appel active 175 , 184
Variante TFE active 181
Vérification à partir d'une liste de blocage des certificats (CRL) 44
Vérification de la route de retour 285
Vérifier PIN 191
Vitesse de chargement maximale 225 , 229 , 273
VLAN 254
Volume 165
Walled Garden 393
Walled Network / Masque réseau 393
Wildcard 356
Zone GEO surveillée 367
Zones 151
Abréviation du numéro 172
Accès distant (p.ex. Follow me, surveillance de la pièce) 12
Action 60 , 168 , 406 , 428 , 431
Actions journalisées 337
Activer IPSec 306
Activer le serveur 365
Activer VLAN 202
Adaptation GRE-Window 326
Adresse de l'expéditeur 194
Adresse distante 432
Adresse e-mail 420
Adresse IP 432
Adresse IP de destination 209
Adresse IP distante 428 , 428
Adresse IP locale 428
Adresse locale 432
Adresse MAC 410 , 431
Adresse physique 432
Affectation de licence 188
Afficher les mots de passe et la clé en clair 12
Agents affectés 174
Agents connectés 174
Agents en post-traitement 174
Algorithme de sécurité 428
Algorithmes d'encryptage 27
Algorithmes de hachage 27
Anciens appels 192
Annonce 425
Aperçu 174
Appareil SMS 421
Appareil terminal 425
Appel direct 17 , 425
Appel en attente 174
Appel en parallèle 425
Appels actifs 174
Appels manqués aujourd'hui 174
Appels reçus aujourd'hui 174
Applications 110
ARS 149
Attribution des numéros de projet 21
Authentification SMTP 420

Authentification pour connexion PPP 39
Authentification RADIUS dynamique 307
Autorisations 94
Autre inactivité 338
Autres fonctions de rejet 426
BOSS 405
Cache négatif 346
Cache positif 346
Caractéristiques de la prestation 100
Certificat local 354
Charger le logiciel système 411
Classe d'autorisation actuelle 425
Commuter la variante d'appel 426
Comportement par défaut 73
Compression 28
Configuration de base 88 , 96
Confirmer le mot de passe de l'administrateur système 11
Connexion 432
Connexion externe TFE 17
Connexions de contrôle entrantes max via adresse IP distante 326
Contact 4
Contrôle d'accessibilité 428
Coupler les connexions externes 6
Coûts 170 , 425
Cryptage de la configuration 406
Crypté 430
Date 170 , 171 , 427
Demande de certificat 46
Description 60 , 141 , 193 , 410 , 428 , 428 , 431 , 431
Description de l'interface 24
Détails 428
Détection NAT 428
Deuxième serveur horaire 14
Devise 9
Directive de mise à jour de l'heure 14
Durée 170 , 171
Durée de vie 194
Emplacement 4
En tant que serveur DHCP 347
En tant que serveur IPCP 347
En-tête de télécopie 365
Enregistrer les connexions entrantes 172
Enregistrer les connexions sortantes 172
Entrée d'alarme 10
Envoyer 433
Envoyer Initial Contact Message 307
Envoyer la chaîne de certificats 309
Envoyer les CRL 309
Envoyer les Key Hash Payloads 309
Envoyer les payloads de requête de certificat 309
Erreur 428 , 430
Erreur de serveur 353
Erreur Rx 431
Erreur Tx 431
État 59 , 60 , 63 , 411 , 425 , 428 , 429 , 431 , 432
Etat de la clé DSA 28
Etat de la clé RSA 28
État du pare-feu 337
État IGMP 248
État UPnP 390
État/État de mise à jour 410
Exporter les donnée de connexion 173
Facteur d'unité de tarification 9
Filtrage complet 337
Fonction 59 , 63
Format de journal 417
Général 113 , 125 , 129 , 162 , 175 , 181
Groupe Pick-Up 21
Groupes maxi 248
Heure 170 , 171 , 427
Heure locale actuelle 14
Horloge d'enregistrement de l'appareil terminal 78
Hôte pour plusieurs sites 396
ID distante 428
ID locale 428
Ignorer les payloads de requête de cer-

tificat 309
IKE (Phase-1) 430
IKE (Phase-1) SAs 428
Imprimer les données de connexion via Serial 2 172
Inactivité PPTP 338
Inactivité TCP 338
Inactivité UDP 338
Inclure les certificats et les clés 406
Indicatif 21
Information sur les taxes (extension S0/Upn) 9
Interface 170 , 171 , 201 , 209 , 210 , 390 , 432 , 433
Interface alternative pour recevoir le serveur DNS 346
Interface de configuration 24
Interface/Emplacement 141
Interphone 425
Interrogations répondues avec succès 353
Intervalle de mise à jour de l'heure 14
Intervalle Schedule 384
IPSec (Phase-2) 430
IPSec (Phase-2) SAs 428
IPSec via TCP 307
IPSec-Debug-Level 306
L'interface est contrôlée UPnP 390
Langue 188 , 193
Langue d'affichage 7
Ligne 174
Logique du système 405
Loopback actif 211
Lu - Di 151
Masque réseau 209
Message 427
Messages 428
Méthode d'authentification 428
Méthode de numérotation 60
Métrique 209
Mettre à jour immédiatement 410
Mettre à jour le logiciel système 412
Mise à jour autorisée 410
Mode 210 , 248
Mode / Groupe Bridge 24
Mode négociation 428
Mot de passe 406 , 420
Mot de passe de l'administrateur système 11
Mot de passe pour accès web 170 , 172 , 179
Mot de passe SMTP 194
MSN par défaut 59
MTU 428
NAT 431
NAT actif 211
Niveau 427
Niveau de journalisation 28
Niveau de routage 149
Niveau maximal de messages des entrées de journal système 4
Nom 59 , 60 , 63 , 169 , 425 , 426
Nom de domaine 346
Nom de fichier actuel sur le flash 406
Nom de l'utilisateur 420 , 432
Nom de l'utilisateur SMTP 194
Nom de l'utilisateur pour accès web 170 , 172 , 179
Nom du fichier 406
Nom du fichier de destination 406
Nom du fichier source 406
Nom du système 4
Nombre maximal d'entrées de journal Accounting 4
Nombre maximal d'entrées de journal Syslog 4
Nombre maximal d'e-mail par minute 420
Nombre maximal de connexions simultanées 26
Nombre maximal de messages d'état IGMP 248
Non modifié depuis 431
Notification 188
Nouveau nom du fichier 406
Nouveaux appels 192
Numéro d'appel sortant 91

Numéro d'appel (MSN) 192 , 425 , 426
Numéro d'appel composé 170
Numéro d'appel externe 171
Numéro d'appel interne 188 , 193 , 412
Numéro de projet 170 , 171
Numéro de téléphone 169
Numéros d'appel 91 , 127 , 151
Numéros d'appel internes 141
Numérotation abrégée 21
N° 210 , 411 , 427 , 431
N° appel int. 170 , 171
Occupé par occupé (Busy on Busy) 426
Octets 428
Octets Rx 431 , 431
Octets Tx 431 , 431
Ouverture/fermeture de session 120 , 177
Paquet DNS invalide 353
Paquets 428
Paquets DNS reçus 353
Paquets Rx 431 , 431
Paquets Tx 431 , 431
Paramètres 127 , 132
Paramètres DSCP pour données SIP 79
Passerelle 209
Pick-Up ciblé 21
PIN1 12
PIN2 12
Plage horaire 14
Port de destination UDP 319
Port distant 428 , 432
Port HTTPS-TCP 354
Port local 428 , 432
Port RTP 78
Port serveur SMTP 194
Port SNMP-Listes-UDP 30
Port SNMP-Trap-UDP 422
Port SSH 26
Port Switch 55
Port TCP du serveur CAPI 365
Port UPnP TCP 390
PPTP-Passthrough 211
Préfixe international/Indicatif pays 7
Préfixe national/Indicatif réseau local 7
Premier serveur horaire 14
Prise d'appel automatique 425 , 426
Protection d'appel (silence) 425
PVID 201
Questions ouvertes 18 , 21
Queue QoS 433
Queued 433
Réglage de l'heure 14
Réglage du pays 7
Régler la date 14
Rejet en absence de réponse 426
Rejet global 10 , 10
Rejet individuel de l'abonné 10
Rejet optionnel 93
Rejet sans notification 211
Rejet sur l'annonce 10
Rejet vers un numéro d'appel 6
Rejeté 430 , 433
Rejeter les non-membres 201
Rejeter les frames sans balise 201
Répondre à la requête du client 390
Requêtes DNS 353
Requêtes transférées 353
Réseaux distants 428
Restaurer les paramètres de base 25
Résultat cache 353
Routage multicast 245
Route étendue 209
Sélection de l'interface Ethernet 55
Sélection de port source UDP 319
Sélection manuelle du groupage 21
Sélectionner le fichier 168 , 406
Séparateur 168
Serveur DHCP primaire 363
Serveur DHCP secondaire 363
Serveur horaire RNIS 14
Serveur POP3 420
Serveur SMTP 194 , 420
Serveur WINS 346

Service de notification 420
Service SSH actif 26
Signal appel en attente 425
Signaler 426
Signalisation de la transmission 6
Signalisation groupée 10
Signalisation TFE 10
SNMP Read Community 12
SNMP Trap Broadcasting 422
SNMP Write Community 12
SNMP-Trap-Community 422
Source 406
Sources maxi 248
Sous-système 427
Supprimer 209
Supprimer la configuration IPSec complète 306
Supprimer le répertoire téléphonique 170
Supprimer les données de connexion 173
Surveillance de la pièce 425
Synchroniser SAs avec l'état de l'interface ISP 307
Système boîte vocale 193
Système en tant que serveur horaire 14
Taille du cache 346
Taille du Zero Cookies 307
Taille GRE-Window 326
Taux de résultat cache (%) 353
TCP-Keepalives 28
Temps de tolérance à la connexion 28
Timeout POP3 420
Total 430
Transfert de communication sans annonce (UbA) 18
Transfert de port 211
Transfert des appels (AWS) 425 , 426
Transfert des appels (CFNR) 17
Transmis 430
Transmission à l'abonné occupé 6 , 18
Troisième serveur horaire 14
TTL maximal pour entrées cache négatives 346
TTL maximal pour entrées cache positives 346
Tunnel IPSec 429
Type 431
Type de routes 209
Type de téléphone 141 , 410 , 411
URL 406
Utilisateur 170 , 171 , 188 , 192
Utilisateurs affectés/Utilisateurs connectés 426
Utilisateurs affectés 427
Utiliser des Zero Cookies 307
Variante 115 , 187
Variante 1 - 4 162 , 176
Variante active (jour) 426
Variante d'appel active 188
Variante d'appel TFE 1 et 2 182
Vérification de la route de retour 210
Version 411
Version de la carte SD 410
Version SNMP 30
Version Téléphone 410
VID de gestion 202
Vitesse actuelle/Mode actuel 55
Vitesse configurée/Mode configuré 55
Actions 372
Administration 202
Affectation des appels 120
Affectation des interfaces 239 , 402
Agents 178
Analogue 137
Aperçu 141
Appel direct 143
Appel en parallèle 111
Applications du rejet 162
Boîtes vocales 188
Cache 352
CAPI 140
Carte mémoire 3

Chaînes de règles 237
Classes d'autorisation 96
Classification QoS 222
Codes modifiables 20
Configuration des routes IPv4 203
Configuration DHCP 359
Configuration du port 55 , 201
Configuration NAT 212
Configuration pool d'adresses IP 358
Connexions 80
Contrôle de numérotation 146
CRL 51
Date 13
Date système 2
Déclencheur 367
Dernière configuration enregistrée 2
Description - Information de connexion - Lien 4
Destinataire de la notification 418
Emplacements 73
Entrant 171
Entrées 167
État 174 , 192
État Service de nuit 2
Extension de domaine 351
Fichiers du logiciel système 411
Fichiers wave 164
Filtre d'accès 234
Filtre QoS 219
Filtre Wake-On-LAN 397
Fonctions de rejet 158
Fournisseur DynDNS 356
Fournisseur SIP 64
FXO 60
FXS 63
Général 149 , 169 , 172 , 179 , 193 , 390
Gigaset Téléphone 125 , 409
Groupage 85
Groupes 338 , 340 , 343
Groupes Drop-In 240
Heure 13
Horloge 17
Hôtes 384
Hôtes statiques 350
HTTP 25
HTTPS 25
Identifiant RNIS 25
Importation / Exportation 168
Interface - Information de connexion - Lien 3
Interfaces 24 , 196 , 387 , 389 , 417
Interfaces NAT 211
Interfaces régulées 273
Interfaces/Directives QoS 225
Interfaces/Fournisseurs 150
IPSec-Peers 276
Jours fériés 157
Liaison IP/MAC 362
Licences système 19
Lignes 175
Liste d'adresses 339
Liste de certificat 44
Liste de services 341
Messages système 427
Mise à jour DynDNS 355
Module DSP 3
Mots de passe 10
Numéro d'appel prioritaire 148
Numéro de série 2
Numéros d'appel 83
Options 39 , 78 , 210 , 248 , 306 , 318 , 326 , 337 , 365 , 383 , 396 , 404 , 417
Options SNMP-Trap 422
Paramètres 412
Paramètres de notification 420
Paramètres DHCP-Relay 363
Paramètres globaux 346
Passerelle hotspot 393
Ping 25
Ping-Generator 388
Pool IP 272 , 306 , 327
PPPoE 254
PPTP 259
Profils Codec 75
Profils de tunnels 310
Profils Phase-1 291

Profils Phase-2 299
Profils XAUTH 304
QoS 336
RADIUS 30
Redémarrage système 413
Règles de filtre 333
Règles WOL 400
Rejet si numérotation erronée 123
RNIS 136 , 263
RNIS externe 57
RNIS interne 58
Routage 151
Serveur de certificat 52
Serveur DNS 348
Serveur HTTPS 354
Serveur Syslog 414
Sessions actives (SIF, RTP, etc...) 3
Signalisation TFE 181
SNMP 25 , 29
SNMP-Trap-Hosts 423
Sortant 170
Ssauvegarde de la configuration sur la carte SD 2
SSH 25 , 26
Statistiques 353 , 430
Statistiques IPSec 429
Système 4
Tableau de routage IPv4 209
TACACS+ 36
Teams 426
Telnet 25
Test DNS 403
Test Ping 403
Test Traceroute 403
Transfert des appels (AWS) 144
Tunnel GRE 328
Tunnel IPSec 428
Tunnel IPSec actif 3
Tunnel PPTP 319
Uptime 2
Utilisateur 42 , 88 , 313 , 364 , 425
Utilisation CPU 3
Utilisation de la mémoire vive 3
Version BOSS 2
VLAN 200
VoIP 132
X.31 86
Zones 151
Accès à la configuration 39
Accès administratif 25
Adaptateur TFE 179
Adresses 339
Appels d'alarme 184
Application vocale 163
Authentification distante 30
Autres téléphones 132
Calendrier 153
Centre d'appel mini 174
Certificats 43
Client DynDNS 354
Codes 20
Configuration IP 196
Connexions externes 80
Diagnostic 403
Directives 333
DNS 344
Données de connexion 170
Drop-In 240
État 2
Général 245
Gigaset Téléphone 125
GRE 328
Groupes 112
HTTPS 353
IGMP 245
Information d'état 425
Interfaces 338 , 430
Internet + composer 251
IP-Accounting 416
IPSec 275 , 428
Journal interne 427
Journal système 414
L2TP 310
Logiciel et configuration 404
Mise à jour du téléphone système 409
Mode Interface / groupes Bridge 22
NAT 211

Paramètres 64
Paramètres de l'utilisateur 88
Paramètres globaux 4
Passerelle hotspot 391 , 432
Ports analogiques 60
Ports Ethernet 54
Ports RNIS 56
PPTP 319
QoS 219 , 432
Real Time Jitter Control 273
Redémarrage 412
Règles d'accès 232
Règles de sélection 148
Rejet 157
Répartition des appels 120
Répertoire téléphonique du système 165
Routes 203
Scheduling 366
Serveur CAPI 364
Serveur DHCP 358
Service de notification 418
Services 340
Services sortants 143
SNMP 422
Surveillance 384
Système boîte vocale 187
Teams 112
Transférer 249
UPnP 389
VLAN 200
Wake-On-LAN 397
Appareil terminal 125
Applications 153
Assistants 1
Contrôle d'appel 143
Création de rapports externe 414
Gestion du système 2
Interfaces 54
Interfaces physiques 54
LAN 196
Maintenance 403
Monitoring 425
Multicast 243
Numérotation 80
Pare-feu 331
Réseau 203
Services locaux 344
VoIP 64
VPN 275
WAN 251
Gigaset DECT 128

A

ACCESS_ACCEPT 31
ACCESS_REJECT 31
ACCESS_REQUEST 31
ACCOUNTING_START 31
ACCOUNTING_STOP 31

N

Numéros d'appel 131

P

Profils d'accès 40